Lectures On Galois Groups and Fundamental Groups

Tamás Szamuely, notes by Francesco Minnocci

Contents

1 Galois theory of fields

1.1 Basic notions

Let k be a field, and consider an algebraic field extension $L|k$. We denote by $\mathrm{Aut}_k(L)$ the group of field automorphisms of L fixing k elementwise, and if $G = \mathrm{Aut}_k(L)$ then we denote by L^G the subfield of elements of L which are fixed under the action of G, that is

$$L^G = \{x \in L \colon \sigma(x) = x \text{ for all } \sigma \in G\}.$$

Definition 1.1. In the above situation, we say that the extension $L|k$ is *Galois* if

$$L^G = k.$$

Recall that an *algebraic closure* of k is an algebraic extension $\overline{k}$ of k that does not admit algebraic extensions other than itself. We now recall the following well-known results from field theory.

Facts 1.2. Let k be a field.

1. There exists an algebraic closure $\overline{k}$ of k.
2. If $L|k$ is an algebraic extension, then there exists an embedding $L \hookrightarrow \overline{k}$ leaving k fixed elementwise.
3. If $\overline{L}$ is a fixed algebraic closure of L, then every embedding $L \hookrightarrow \overline{k}$ fixing k extends to an isomorphism $\overline{L} \xrightarrow{\sim} \overline{k}$.

For a proof, we refer to [1, Chapter V - 2.6 & 2.8].

Definition 1.3. Let $L|k$ be an algebraic field extension.

- An element x in L is *separable* over k if the minimal polynomial of x over k has no multiple roots.
- The extension $L|k$ is *separable* if every element of L is separable over k.

Definition 1.4. Let k be a field and let $\overline{k}$ be a fixed algebraic closure of k. The *separable closure* of k in $\overline{k}$ is

$$k_s = \{\lambda \in \overline{k} \colon \lambda \text{ is separable over } k\}.$$

The *absolute Galois group* of k is

$$\mathrm{Gal}(k_s|k) = \mathrm{Aut}_k(k_s).$$

Remark 1.5.

1. The extension $k_s|k$ is Galois. In fact, it suffices to show that for every element x in k_s not contained in k there exists an automorphism σ in $\mathrm{Gal}(k_s|k)$ such that $\sigma(x) \neq x$. Let x' be another root of the minimal polynomial of x over k. Then the assignment $x \mapsto x'$ induces a field isomorphism $k(x) \xrightarrow{\sim} k(x')$ that fixes k elementwise. By Fact 1.2 (3), the latter extends to an automorphism $\sigma\colon \overline{k} \to \overline{k}$. Since σ sends each element to another root of its minimal polynomial over k, it maps k_s onto itself, determining an automorphism of k_s which sends x to x'.

2. The absolute Galois group of k depends on the choice of the algebraic closure $\overline{k}$ of k.

Proposition 1.6. Let $L|k$ be a separable field extension and let k_s be a separable closure of L. The following are equivalent.

1. $L|k$ is a Galois extension.

2. The minimal polynomial over k of each element of L splits into linear factors in L.

3. Each σ in $\mathrm{Gal}(k_s|k)$ satisfies $\sigma(L) \subseteq L$.

Recall that an extension $L|k$ satisfying property (3) of Proposition 1.6 is called a *normal* extension.

Proof. First, we prove (1) $\Rightarrow$ (2). Let x be an element in L. Then x is a root of the polynomial

$$f = \prod_{\sigma \in S} (t - \sigma(x)),$$

where S is a system of coset representatives of the stabilizer of x in $\mathrm{Gal}(k_s|k)$. Let g be the minimal polynomial of x over k. Then $\sigma(x)$ is a root of g for all σ in S, so f divides g. Since g is irreducible and monic, we conclude $f = g$.

The implication (2) $\Rightarrow$ (3) is trivial, so we prove (3) $\Rightarrow$ (1). Let x be an element in $L \setminus k$. Since $k_s|k$ is a Galois extension, x is moved by some σ in $\mathrm{Gal}(k_s|k)$. As $\sigma(L) \subseteq L$, σ restricts to an element of $\mathrm{Aut}_k(L)$ which does not fix x. $\square$

Here is an important result which allows us to characterize infinite extensions in terms of their finite subextensions:

Fact 1.7. If $L|k$ a finite separable extension, then there exists a finite Galois extension $M|k$ containing L.

It essentially follows from the Primitive Element Theorem, by taking the splitting field of the minimal polynomial of a generator of the extension.

Corollary 1.8. If $L|k$ is an infinite Galois extension, then L is the union of its finite Galois subextensions:

$$L = \bigcup_{\substack{k \subseteq M \subseteq L \\ M \text{ finite Galois}}} M.$$

We want to reduce questions about infinite Galois theory to the finite case: let $L|k$ be an infinite Galois extension and consider two finite Galois subextensions $L_1 \subset L_2 \subset L$ over k. Then there are surjective restriction maps

$$\mathrm{Gal}(L_2|k) \twoheadrightarrow \mathrm{Gal}(L_1|k),$$

and the idea is to "pass to the limit" in L_2. To make this precise, we need to introduce the notion of profinite groups.

1.2 Profinite groups and their topology

Definition 1.9. A (filtered) inverse system of groups $(G_\alpha, \varphi_{\alpha\beta})_{\alpha,\beta\in\Lambda}$ consists of

- a partially ordered set $(\Lambda, \leq)$ that is *directed*, i.e. for every α, β in Λ there exists γ in Λ such that $\alpha \leq \gamma$ and $\beta \leq \gamma$;
- a group G_α for each α in Λ;
- A group homomorphism $\varphi_{\alpha\beta}\colon G_\beta \to G_\alpha$ for every $\alpha \leq \beta$ in Λ such that
  - $\varphi_{\alpha\alpha} = \mathrm{id}_{G_\alpha}$ for all α in Λ;
  - $\varphi_{\alpha\gamma} = \varphi_{\alpha\beta} \circ \varphi_{\beta\gamma}$ for all $\alpha \leq \beta \leq \gamma$ in Λ.

Definition 1.10. The *inverse limit* of an inverse system of groups $(G_\alpha, \varphi_{\alpha\beta})_{\alpha,\beta\in\Lambda}$ is the subgroup of the direct product $\prod_{\alpha\in\Lambda} G_\alpha$

$$\varprojlim_{\alpha\in\Lambda} G_\alpha = \left\{ (g_\alpha) \in \prod_{\alpha\in\Lambda} G_\alpha \colon \varphi_{\alpha\beta}(g_\beta) = g_\alpha \text{ for all } \alpha \leq \beta \right\}.$$

Definition 1.11 (Profinite group)**.** A *profinite group* is an inverse limit of a (filtered) inverse system of finite groups.

Example 1.12.

1. Every finite group is profinite (it is the limit of the constant system).
2. Let G be a group, and consider the set

   $$\Lambda = \{U \lhd G : \; [G\colon U] < \infty\},$$

   of normal subgroups of finite index, ordered by reverse inclusion. For $U \subset V$ in Λ we have projection maps $\varphi_{UV}\colon G/V \twoheadrightarrow G/V$, and the resulting inverse limit

   $$\widehat{G} = \varprojlim_{U\in\Lambda} G/U$$

   is called the *profinite completion* of G.

3. Taking $G = \mathbf{Z}$ in the previous example, we obtain the profinite completion of the integers

$$\widehat{\mathbf{Z}} = \varprojlim_{n \in \mathbf{N}} \mathbf{Z}/n\mathbf{Z}.$$

Here the reduction maps are given by $\mathbf{Z}/n\mathbf{Z} \twoheadrightarrow \mathbf{Z}/m\mathbf{Z}$ for $m \mid n$. In fact, $\widehat{\mathbf{Z}}$ is also a ring with componentwise multiplication.

Exercise 1.13. Show that there is an isomorphism

$$\widehat{\mathbf{Z}} \cong \prod_{p \text{ prime}} \mathbf{Z}_p.$$

Here, $\mathbf{Z}_p = \varprojlim_n \mathbf{Z}/p^n\mathbf{Z}$ is the additive group of p-adic integers. Again, $\mathbf{Z}_p$ is also a ring and the above turns out to be an isomorphism of rings.

Fix a profinite group $G = \varprojlim_{\alpha \in \Lambda} G_\alpha$. We can equip each G_α with the discrete topology, the direct product $\prod_{\alpha \in \Lambda} G_\alpha$ with the product topology, and the inverse limit $G \subseteq \prod_{\alpha \in \Lambda} G_\alpha$ with the subspace topology. The following fact follows directly from the definitions.

Fact 1.14. The projection maps

$$\pi_\alpha \colon G \twoheadrightarrow G_\alpha$$

are continuous for the above topology, and the subgroups $\ker(\pi_\alpha)$ form a basis of open neighborhoods of the identity in G.

Lemma 1.15. The topological group G is a closed subspace of $\prod_{\alpha \in \Lambda} G_\alpha$.

Proof. We prove that the complement is open. Pick $g = (g_\alpha)_{\alpha \in \Lambda}$ not in G. Then there exist $\alpha \leq \beta$ such that $\varphi_{\alpha\beta}(g_\beta) \neq g_\alpha$. The open set

$$\pi_\alpha^{-1}(\{g_\alpha\}) \cap \pi_\beta^{-1}(\{g_\beta\})$$

contains g and is disjoint from G. □

By Tychonoff's theorem, the product $\prod_{\alpha \in \Lambda} G_\alpha$ is compact (and it is obviously Hausdorff), so we get the following.

Corollary 1.16. A profinite group is a compact Hausdorff topological group.

In fact, it can be shown that the profinite structure is determined by purely topological properties:

Fact 1.17. A topological group is profinite if and only if it is compact, Hausdorff and totally disconnected.

For a proof, we refer to [2, Theorem 1.1.12].

1.3 The Galois correspondence

Proposition 1.18. Let $K|k$ be a Galois extension. Then there is a group isomorphism

$$\mathrm{Gal}(K|k) \cong \varprojlim_{L} \mathrm{Gal}(L|k),$$

where L runs over the finite Galois subextensions $L|k$ contained in K. In particular, $\mathrm{Gal}(K|k)$ is a profinite group.

Proof. Consider the restriction map

$$\begin{aligned} \Phi : \mathrm{Gal}(K|k) &\to \varprojlim_{L} \mathrm{Gal}(L|k) \\ \sigma &\mapsto (\sigma|_L)_L \end{aligned}$$

which is well-defined by Proposition 1.6 (3). Then Φ is continuous and injective, as if $\sigma \neq 1$ then there is some α in K such that $\sigma(\alpha) \neq \alpha$; since α is contained in a finite Galois extension $L|k$, we have $\sigma|_L \neq 1$. For surjectivity, given an element $(\sigma_L)_L$ in the limit, we define $\sigma\colon K \to K$ by $\sigma(\alpha) = \sigma_L(\alpha)$ where $L|k$ is a finite Galois extension containing α. Note that σ is well-defined, as if $L' \supseteq L$ is another such extension then $\sigma_{L'}|_L = \sigma_L$. It is easy to see that σ is a field automorphism of K fixing k elementwise, and by construction $\Phi(\sigma) = (\sigma_L)_L$. □

Corollary 1.19. For every finite Galois extension $L|k$ contained in K there is a continuous surjection

$$\mathrm{Gal}(K|k) \twoheadrightarrow \mathrm{Gal}(L|k).$$

Proof. The desired map is the continuous homomorphism making the diagram

$$\begin{array}{ccc} \mathrm{Gal}(K|k) & \longrightarrow & \prod_L \mathrm{Gal}(L|k) \\ & \searrow & \downarrow \pi_L \\ & & \mathrm{Gal}(L|k) \end{array}$$

commute. This is surjective because every automorphism σ of $L|k$ extends to an automorphism $\widetilde{\sigma}$ of the separable closure k_s, and the latter restricts to an automorphism of $K|k$ which is sent to σ by the above map. □

Example 1.20.

1. Let $\mathbf{F}$ be a finite field and let $\mathbf{F}_s$ be its separable (algebraic) closure. If $L|\mathbf{F}$ is a finite extension of degree n, then it is Galois with cyclic Galois group of order n. These assemble to an isomorphism
$$\mathrm{Gal}(\mathbf{F}_s|\mathbf{F}) \cong \widehat{\mathbf{Z}}.$$
If $|\mathbf{F}| = q$, then the isomorphism is given by sending the Frobenius automorphism $x \mapsto x^q$ to $1 \in \widehat{\mathbf{Z}}$, which generates a dense subgroup $\mathbf{Z} \subseteq \widehat{\mathbf{Z}}$.

2. Take $k = \mathbf{C}((t))$. Then, by a theorem of Puiseux, every finite Galois extension of k is given by adjoining the n-th root of t for some n, and thus

$$\mathrm{Gal}(\overline{\mathbf{C}((t))}|\mathbf{C}((t))) \cong \widehat{\mathbf{Z}}.$$

3. Fix a prime number p, and let $k = \mathbf{Q}(\mu_{p^\infty}) = \bigcup_{r\geq 1} \mathbf{Q}(\mu_{p^r})$ be the extension of $\mathbf{Q}$ obtained by adjoining all p-power roots of unity. By a well-known result from number theory, each term has Galois group

$$\mathrm{Gal}(\mathbf{Q}(\mu_{p^r})|\mathbf{Q}) \cong (\mathbf{Z}/p^r\mathbf{Z})^\times,$$

and taking the limit we get an isomorphism

$$\mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})|\mathbf{Q}) \cong \mathbf{Z}_p^\times,$$

where we used the fact that the units of the finite rings $(\mathbf{Z}/p^r\mathbf{Z})^\times$ assemble to the units of the inverse limit $\mathbf{Z}_p$. Finally, if $\mathbf{Q}(\mu) = \bigcup_{n\geq 1} \mathbf{Q}(\mu_n)$ is obtained by adjoining all roots of unity, then

$$\mathrm{Gal}(\mathbf{Q}(\mu)|\mathbf{Q}) \cong \widehat{\mathbf{Z}}^\times.$$

Now we are ready to state and prove the main result of Galois theory for arbitrary Galois extensions.

Theorem 1.21. Let $K|k$ be a Galois extension and let L be a subextension of $K|k$. Then $\mathrm{Gal}(K|L)$ is a closed subgroup of $\mathrm{Gal}(K|k)$, and the assignments

$$L \longmapsto H = \mathrm{Gal}(K|L)$$
$$H \longmapsto K^H$$

yield an inclusion-reversing bijection

$$\left\{ \text{ subfields } K \supseteq L \supseteq k \right\} \longleftrightarrow \left\{ \text{ closed subgroups } H \leq \mathrm{Gal}(K|k) \right\}.$$

Moreover, finite extensions $L|k$ correspond to open subgroups $H \leq \mathrm{Gal}(K|k)$, and Galois extensions $L|k$ correspond to normal subgroups $H \triangleleft \mathrm{Gal}(K|k)$.

Remark 1.22.

- In a topological group, every open subgroup is closed, since its complement is a union of the other open cosets. In fact, they are precisely the closed subgroups of finite index in any compact topological group.
- If $K|k$ is an infinite Galois extension, there may exist non-closed subgroups in $\mathrm{Gal}(K|k)$, for example $\mathbf{Z}$ is a dense subgroup of $\widehat{\mathbf{Z}} \cong \mathrm{Gal}(\overline{\mathbf{F}}_p|\mathbf{F}_p)$. In general, we can use the following idea of Dedekind: take an infinite chain

$$k = k_0 \subsetneq k_1 \subsetneq k_2 \subsetneq \ldots \subsetneq K$$

and if $k_i \neq k_{i+1}$, one proves that every σ in $\mathrm{Gal}(k_i|k)$ extends to $\widetilde{\sigma}$ in $\mathrm{Gal}(k_{i+1}|k)$ in at least two ways, which implies that $\mathrm{Gal}(K|k)$ is uncountable. Similarly, one shows that a closed subgroup $H \leq \mathrm{Gal}(K|k)$ is uncountable, and thus countable subgroups are never closed.

The following theorem indicates that the absolute Galois group of a field encodes a lot of information about the field itself; the number field case was proven by Neukirch in 1969.

Theorem 1.23 (Pop, 1994)**.** Let K_1, K_2 be finitely generated field extensions of $\mathbf{Q}$. If there is an isomorphism of topological groups

$$\Phi : \mathrm{Gal}(\overline{K}_1|K_1) \xrightarrow{\sim} \mathrm{Gal}(\overline{K}_2|K_2),$$

then $K_1 \xrightarrow{\sim} K_2$ as fields. In fact, every such isomorphism comes from an isomorphism of the algebraic closures $\varphi\colon \overline{K}_1 \xrightarrow{\sim} \overline{K}_2$ by conjugation: $g \mapsto \varphi \circ g \circ \varphi^{-1}$.

We now start proving Theorem 1.21, dividing the proof into several steps.

Proposition 1.24. Let $K|k$ be a Galois extension and let L be an intermediate field extension of $K|k$. Then $\mathrm{Gal}(K|L)$ is a closed subgroup of $\mathrm{Gal}(K|k)$.

Proof. We first assume that L/k is a finite subextension, and show that $\mathrm{Gal}(K|L)$ is open in $\mathrm{Gal}(K|k)$. Since L embeds in some finite Galois extension M of k contained in K, there is a continuous surjection

$$\varphi_M : \mathrm{Gal}(K|k) \twoheadrightarrow \mathrm{Gal}(M|k) \supset \mathrm{Gal}(M|L)$$

and $U_L \coloneqq \varphi_M^{-1}(\mathrm{Gal}(M|L)) \subset \mathrm{Gal}(K|k)$ is open. Also, we have an inclusion $\mathrm{Gal}(K|L) \subseteq U_L$ because its image in $\mathrm{Gal}(M|k)$ is exactly $\mathrm{Gal}(M|L)$, so it suffices to show the reverse inclusion: if σ is an element in U_L, then $\sigma|_M$ lies in $\mathrm{Gal}(M|L)$, so $\sigma|_L = \mathrm{id}_L$ and thus σ lies in $\mathrm{Gal}(K|L)$. Thus $\mathrm{Gal}(K|L) = U_L$ is open. If L is arbitrary, then $L = \bigcup_{\alpha\in\Lambda} L_\alpha$ where L_α ranges over the finite Galois extensions of k contained in L. Then,

$$\mathrm{Gal}(K|L) = \bigcap_{\alpha\in\Lambda} \mathrm{Gal}(K|L_\alpha)$$

is an intersection of open subgroups (which are always closed), hence closed. □

Proposition 1.25. The assignment $L \mapsto \mathrm{Gal}(K|L)$ induces an inclusion-reversing bijection between subextensions of $K|k$ and closed subgroups of $\mathrm{Gal}(K|k)$, whose inverse is given by $H \mapsto K^H$.

Proof. The previous proposition implies that the map $L \mapsto \mathrm{Gal}(K|L)$ is well-defined. Moreover, if $H = \mathrm{Gal}(K|k)$ is the whole group, then $K^H = L$ because $K|L$ is Galois.

Now let H be a closed subgroup of $\mathrm{Gal}(K|L)$, and set $L \coloneqq K^H$. We want to show that they are in fact equal. Pick σ in $\mathrm{Gal}(K|L)$ and consider intermediate finite Galois extensions $K \supseteq M \supseteq L$. Then the groups $U_M = \mathrm{Gal}(K|M)$ for varying M form a basis of open neighborhoods of the identity in $\mathrm{Gal}(K|L)$, and the subgroup $H \leq \mathrm{Gal}(K|L)$ surjects onto $\mathrm{Gal}(M|L)$ via the natural projection φ_M (because any element not contained in L is moved by some element of H). So, there exists some τ in H such that $\varphi_M(\tau) = \varphi_M(\sigma)$. In other words, $H \cap \sigma(U_M) \neq \emptyset$ for every M, but H is closed, so σ lies in H and we are done. □

Proposition 1.26. In the above correspondence, finite extensions $L|k$ correspond to open subgroups $H \leq \mathrm{Gal}(K|k)$, and Galois extensions $L|k$ correspond to normal subgroups $H \triangleleft \mathrm{Gal}(K|k)$.

Proof. Suppose that H is a normal subgroup of G and set $L = K^H$. Then G/H acts on L and $L^{G/H} = (K^H)^{G/H} = K^G = k$, so $L|k$ is Galois.

Conversely, if $L|k$ is Galois, then there exists a homomorphism $G \to \mathrm{Gal}(L|k)$ with kernel $H = \mathrm{Gal}(K|L)$, which is thus normal in G. □

1.4 Grothendieck's Galois theory

Fix a base field k and a separable closure k_s of k. Consider the assignment

$$L \mapsto \mathrm{Hom}_k(L, k_s)$$

which sends a finite separable extension of k to the set of k-algebra homomorphisms $L \to k_s$. This is a finite set: if $L = k(\alpha)$ and f is the minimal polynomial of α over k, every such homomorphism is determined by the image of α, which must be a root of f in k_s. Note that there is a left action of $G_k \coloneqq \mathrm{Gal}(k_s|k)$ on $\mathrm{Hom}_k(L, k_s)$ by

$$\begin{aligned} G_k \times \mathrm{Hom}_k(L, k_s) &\to \mathrm{Hom}_k(L, k_s) \\ (\sigma, \varphi) &\mapsto \sigma \circ \varphi \,. \end{aligned}$$

Definition 1.27. If G is a topological group acting on a discrete set X, we say that the action is *continuous* if the map

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

is continuous.

Lemma 1.28. In the above situation, the action of G on X is continuous if and only if the stabilizer of every x in X is open in G.

Proof. Take an element x in X and consider the fibre

$$G_x = \{g \in G \colon g \cdot x = x\}$$

of x under the composition

$$G \xrightarrow{(id,x)} G \times X \to X.$$

If $G \times X \to X$ is continuous, then G_x is open. On the other hand, suppose G_x is open for all x in X. We prove that the fibre

$$U_x = \{(g, y) \in G \times X \colon g \cdot y = x\} \subset G \times X$$

is open. We can write

$$U_x = \bigsqcup_{y \in X} \{(g, y) \in G \times \{y\} : \ g \cdot y = x\}$$

and each of the sets in the disjoint union is either empty or homeomorphic to G_x, hence U_x is open. ☐

Proposition 1.29. If $L|k$ is a finite separable extension, then the finite set $\mathrm{Hom}_k(L, k_s)$ is equipped with a continuous and transitive G_k-action.

Proof. The action is continuous because the stabilizer of any element φ of $\mathrm{Hom}_k(L, k_s)$ is equal to $\mathrm{Gal}(k_s|\varphi(L))$, which is open in G_k as it is closed and of finite index.

For transitivity, notice that $\mathrm{Gal}(k_s|k)$ permutes the roots of the minimal polynomial of any element of L transitively. ☐

Suppose now $M|k$ is another finite separable extension, and let $\rho : L \to M$ be a k-algebra homomorphism. Then ρ induces a map

$$\rho^* : \mathrm{Hom}_k(M, k_s) \to \mathrm{Hom}_k(L, k_s)$$
$$\varphi \mapsto \varphi \circ \rho$$

which is compatible with the action of G_k. In other words, we have defined a *contravariant* functor from the category of finite separable extensions of k to the category of finite sets with continuous transitive G_k-action.

Definition 1.30. Two categories $\mathcal{C}$ and $\mathcal{D}$ are *equivalent* if there exist two functors

$$F : \mathcal{C} \to \mathcal{D}, \quad G : \mathcal{D} \to \mathcal{C}$$

such that $F \circ G$ and $G \circ F$ are naturally isomorphic to the identity functors of $\mathcal{D}$ and $\mathcal{C}$, respectively. An anti-equivalence of categories is an equivalence between $\mathcal{C}$ and the opposite category $\mathcal{D}^{\mathrm{op}}$ of $\mathcal{D}$.

Example 1.31. Let $\mathcal{D}$ be the category of finite-dimensional vector spaces over a field k, and let $\mathcal{C}$ be the category of vector spaces of the form k^n for some n in $\mathbf{N}$. There is an obvious functor $F\colon \mathcal{C} \to \mathcal{D}$ sending k^n to itself; it induces an equivalence of categories: to define $G\colon \mathcal{D} \to \mathcal{C}$, we need to fix a k-basis of each vector space in $\mathcal{D}$. This induces an isomorphism $V \xrightarrow{\sim} k^n$ for $n = \dim_k(V)$. We set $G(V) := k^n$ and we the image of a morphism via G as the associated matrix with respect to the chosen bases. This highlights the two main features of equivalences of categories: the objects of the two categories are only in bijection "up to isomorphism", while "locally" the morphisms are the same, meaning that for every two objects there is a bijection between the sets of morphisms.

Theorem 1.32. The functor $L \mapsto \mathrm{Hom}_k(L, k_s)$ induces an anti-equivalence between the category of finite separable extensions of k and the category of finite sets with continuous transitive G_k-action.

Proof. Omitted, in favor of the more general Theorem 1.35 below. □

Definition 1.33. A k-algebra is *finite étale* if it is isomorphic to a finite direct product of finite separable extensions of k.

Remark 1.34. One can prove the following equivalent characterizations for a finite-dimensional k-algebra A:

$$A \text{ finite étale} \iff A \otimes_k \overline{k} \text{ is reduced} \iff \Omega^1_{A|k} = 0,$$

where $\overline{k}$ is an algebraic closure of k and $\Omega^1_{A|k}$ is the module of Kähler differentials (recall that a k-algebra is reduced if it has no nilpotents).

Theorem 1.35. The contravariant functor $A \mapsto \mathrm{Hom}_k(A, k_s)$ induces an anti-equivalence of categories

$$\left\{ \text{ finite étale } k\text{-algebras } \right\} \longleftrightarrow \left\{ \text{ finite sets with continuous } G_k\text{-action } \right\}.$$

We now explain how to reduce the case of étale k-algebras to the case of field extensions.

Remark 1.36. If A is the direct product $\prod_{i=1}^n L_i$ of finite separable extensions $L_i|k$, then we have an orbit decomposition

$$\mathrm{Hom}_k(A, k_s) \cong \bigsqcup_{i=1}^n \mathrm{Hom}_k(L_i, k_s)$$

which is compatible with the Galois action.

Proof. We show that any $\phi : A \to k_s$ factors through exactly one of the fields L_i, from which the claim follows. Since ϕ is not zero, there exists some i such that the restriction to the subring

$$0 \times \cdots \times L_i \times \cdots \times 0 \subset A$$

is not zero, hence injective as the kernel must be a proper ideal. Similarly, if this were to hold for some other $j \neq i$, then the induced map

$$0 \times \cdots \times L_i \times \cdots \times L_j \times \cdots \times 0 \to k_s$$

would be injective, which is a contradiction since the domain has zero-divisors. Therefore, ϕ defines a homomorphism of fields from the copy of L_i sitting inside A to k_s, which gives the desired factorization (note that the identity of L_i inside A is automatically sent by ϕ to $1 \in k_s$, as the identity of L_j goes to zero for all $j \neq i$). □

The following formal lemma is useful when dealing with equivalences of categories.

Lemma 1.37. Let $F\colon \mathcal{C} \to \mathcal{D}$ be a functor. Then F induces an equivalence of categories if and only if

- F is fully faithful (i.e. for every C, C' in $\mathcal{C}$ the map
$$\mathrm{Hom}_{\mathcal{C}}(C, C') \to \mathrm{Hom}_{\mathcal{D}}(F(C), F(C'))$$
is bijective);
- F is essentially surjective (i.e. for every D in $\mathcal{D}$ there exists some C in $\mathcal{C}$ such that $F(C) \cong D$).

Proof. We only prove the interesting direction, which is the one we shall need. Suppose F is fully faithful and essentially surjective. We have to construct a quasi-inverse $G\colon \mathcal{D} \to \mathcal{C}$: for every object V in $\mathcal{D}$, we fix an isomorphism

$$i_V\colon F(A) \xrightarrow{\sim} V$$

for some object A in $\mathcal{C}$ and set $G(V) := A$. Given a morphism $f\colon V \to W$ in $\mathcal{D}$, we define $G(f)$ via the following commutative diagram:

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ {\scriptstyle i_V}\uparrow{\scriptstyle \cong} & & {\scriptstyle i_W}\uparrow{\scriptstyle \cong} \\ F(A) & \xrightarrow{i_W \circ f \circ i_V^{-1}} & F(B) \end{array}$$

Since F is fully faithful, there exists a unique morphism $g \in \mathrm{Hom}_{\mathcal{C}}(A, B) \overset{1:1}{\longleftrightarrow} \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$ which corresponds to $i_W \circ f \circ i_V^{-1}$, so we set $G(f) := g$.

By construction, we have an isomorphism $i_V\colon F(G(V)) \cong V$ which is compatible with morphisms, so we have to check that $G \circ F \cong \mathrm{id}_{\mathcal{C}}$: for every A in $\mathcal{C}$ we need morphisms

$$G(F(A)) \to A, \quad A \to G(F(A))$$

which are inverse to each other, and by fully faithfulness it suffices to construct morphisms

$$F(G(F(A))) \to F(A), \quad F(A) \to F(G(F(A)))$$

which are inverse to each other: we can just take the isomorphism $i_{F(A)}$ and its inverse. □

Proof of Theorem 1.35. We've already restricted to the case of finite separable extensions $L|k$ and transitive G_k-sets.

For essential surjectivity, suppose S is a finite set endowed with a continuous transitive G_k-action. If s is an element in S, its stabilizer $U_s \subset G_k$ is open by continuity of the action, and so $L = k_s^{U_s}$ is a finite separable extension of k. If $r : L \to k_s$ is the inclusion, by transitivity of the action on $\mathrm{Hom}_k(L, k_s)$ we can define a map

$$\begin{aligned} \mathrm{Hom}_k(L, k_s) &\to S \\ g \circ r &\mapsto g \cdot s, \end{aligned}$$

and by construction it is a G_k-equivariant bijection (everything works because U_s is the stabilizer of r).

For fully faithfulness, given finite separable extensions $L, M|k$ we need to show that the assignment

$$\begin{aligned} \mathrm{Hom}_k(L, M) &\to \mathrm{Hom}_{G_k}(\mathrm{Hom}_k(M, k_s), \mathrm{Hom}_k(L, k_s)) \\ \rho &\mapsto \rho^* \end{aligned}$$

is bijective. Since $\mathrm{Hom}_k(L, k_s)$ and $\mathrm{Hom}_k(M, k_s)$ are transitive G_k-sets, a map

$$f : \mathrm{Hom}_k(M, k_s) \to \mathrm{Hom}_k(L, k_s)$$

is determined by the image of a fixed element φ in $\mathrm{Hom}_k(M, k_s)$. Since f is compatible with the action of G, if U is the stabilizer of φ and V is the stabilizer of $f(\varphi)$, then $U \subseteq V$. But then, we get the the desired map $L \to M$ via the following diagram:

$$\begin{array}{ccc} k_s^V & \hookrightarrow & k_s^U \\ \cong\uparrow & & \cong\uparrow \\ f(\varphi)(L) & \dashrightarrow & \varphi(M) \\ \cong\uparrow & & \cong\uparrow \\ L & \dashrightarrow & M \end{array}$$

□

2 Topological Covers

In this section, we assume all topological spaces to be locally connected.

2.1 Galois theory of Covers

Definition 2.1. Let X be a topological space A *space over* X is a topological space Y together with a continuous map $p : Y \to X$. A morphism of spaces over X is a diagram of continuous maps

$$\begin{array}{ccc} Y & \xrightarrow{f} & Z \\ & {\scriptstyle p_1}\searrow \quad \swarrow{\scriptstyle p_2} & \\ & X & \end{array}$$

A space over X is a *cover* if for every x in X there exists an open neighborhood V of x such that $p^{-1}(V) \cong \bigsqcup_{i \in I} U_i$ and such that the restriction $p|_{U_i} : U_i \xrightarrow{\sim} V$ is a homeomorphism for every i in I.

Example 2.2. If I is a discrete space, then the projection $X \times I \to X$ is the trivial cover with fibre I.

Remark 2.3. $p : Y \to X$ is a cover if and only if for all x in X there exists an open neighborhood V of x such that $p^{-1}(V)$ is isomorphic, as a space over V, to a trivial cover.

Definition 2.4. Let G be a group acting on the left on a topological space X. The action of G is *even* if every x in X has a open neighborhood U such that the open sets gU are pairwise disjoint as g varies in G.

Remark 2.5. If G acts evenly on a space Y, then the natural projection $Y \xrightarrow{p_G} Y/G$ turns Y into a cover of Y/G. Indeed, every x in X has an open neighborhood of the form $p_G(U)$.

Definition 2.6. Let $Y \to X$ be a cover. An automorphism of Y as a cover of X is an automorphism of Y as a space over X. The group of automorphisms of Y as a cover of X is denoted by $\mathrm{Aut}(Y|X)$.

Proposition 2.7. If Y is connected and $\varphi \in \mathrm{Aut}(Y|X)$ has a fixed point, then $\varphi = \mathrm{id}_Y$.

This follows from an elementary fact about covers, of which we omit the proof:

Lemma 2.8. Let $p : Y \to X$ be a cover and let Z be a connected space endowed with two maps $f, g\colon Z \to Y$ such that $p \circ f = p \circ g$. If there exists some $z \in Z$ such that $f(z) = g(z)$, then $f = g$.

Indeed, taking $Z = Y$ and $f = \varphi$ and $g = \mathrm{id}_Y$ we get the previous proposition.

Corollary 2.9. If $Y \xrightarrow{p} X$ is a connected cover, then $\mathrm{Aut}(Y|X)$ acts evenly on Y.

Proof. Pick some y in Y and let V be a connected open neighborhood of $x := p(y)$ such that $p^{-1}(V) \cong \bigsqcup_{i \in I} U_i$, with $y \in U_i$ for some i. Then, the $\varphi(U_i)$ are disjoint and if $\varphi \neq \mathrm{id}$ then it must take U_i to U_j with $j \neq i$, because if $\varphi(U_i) = U_i$ then φ would have a fixed point in U_i and thus be the identity, which is a contradiction. □

Corollary 2.10. If G acts evenly on a connected space Y, then $\mathrm{Aut}(Y|Y/G) = G$.

Proof. The inclusion $G \leq \mathrm{Aut}(Y|Y/G)$ is clear. Conversely, gives $\varphi \in \mathrm{Aut}(Y|Y/G)$, for a fixed y in Y there is some g in G such that $\varphi(y) = g \cdot y$. This means that $\varphi^{-1} \circ g$ has a fixed point, so it is the identity and thus $g = \varphi$. □

Let $Y \xrightarrow{p} X$ be a connected cover, and consider the factorization

$$Y \to Y/\,\mathrm{Aut}(Y|X) \xrightarrow{\overline{p}} X.$$

Definition 2.11. A cover $Y \xrightarrow{p} X$ is *Galois* if $\overline{p}$ is an isomorphism.

Remark 2.12. If $Y \to X$ is a connected cover, then $Y \to X$ is Galois if and only if $\mathrm{Aut}(Y|X)$ acts transitively on the fibres of $Y \xrightarrow{p} X$. This is because the underlying set of $Y/\mathrm{Aut}(Y|X)$ is the set of $\mathrm{Aut}(Y|X)$-orbits of Y, so $\overline{p}$ is a bijection if and only if each orbit is the entire fibre.

Moreover, it is enough that the action is transitive on just *one* fibre. This is because $Y/\mathrm{Aut}(Y|X) \to X$ is a connected cover of X (see the proposition below), and in a connected cover all fibres have the same cardinality.

Theorem 2.13 (Galois Theory for Covers)**.** Let $Y \to X$ be a Galois cover with group $G = \mathrm{Aut}(Y|X)$.
If $H \leq G$ is a subgroup, then $Y/H \to X$ is a connected cover lying between Y and X. Conversely, if $Y \xrightarrow{f} Z$ is a morphism between connected covers of X, then f is itself a Galois cover and $Z \cong Y/H$ with $H = \mathrm{Aut}(Y|Z)$. In this correspondence, normal subgroups $H \triangleleft \mathrm{Aut}(Y|X)$ induce Galois covers $Z \to X$ with

$$\mathrm{Aut}(Z|X) \cong \mathrm{Aut}(Y|X)/H.$$

Let us fix $p\colon Y \to X$ to be a Galois cover. We divide the proof of the theorem into multiple steps.

Proposition 2.14. If $H \leq \mathrm{Aut}(Y|X)$ is a subgroup, then $Y/H \to X$ is a cover.

Proof. We have the following factorization factorization of p:

$$Y \to Y/H \xrightarrow{p_H} X,$$

where p_H is continuous and surjective. Since $Y \to X$ is a cover, over sufficiently small $V \subset X$ we have

$$p^{-1}(V) \cong V \times I$$

for some discrete set I, and thus

$$p_H^{-1}(V) \cong V \times (I/H),$$

which shows that p_H is a cover. □

Proposition 2.15. Suppose we have a map of spaces over X:

$$\begin{array}{ccc} Y & \xrightarrow{\quad p_Y \quad} & Z \\ & {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle p_2} & \\ & X & \end{array}$$

where $Z \to X$ is a connected cover. Then, $Y \to Z$ is a Galois cover.

Lemma 2.16. If $Y \xrightarrow{p_Y} Z \xrightarrow{p_2} X$ are all connected such that $Y \xrightarrow{p} X$ and $Z \to X$ are covers, then $Y \to Z$ is a cover.

Proof. For every z in Z, set $x \coloneqq p_2(z)$ and pick a connected open neighborhood V of x such that

$$p^{-1}(V) \cong \bigsqcup_{i \in I} U_i$$

and

$$p_2^{-1}(V) \cong \bigsqcup_{j \in J} V_j.$$

Then, for every i there exists j such that $p_Y(U_i) = V_j$: indeed, $p_Y(U_i)$ is a connected subset which maps homeomorphically to V via p_2.

Finally, we need to show that p_Y is surjective. Since Z is connected and $p_Y(Y)$ is open, it suffices to show that its complement in Z is also closed. If z is a point outside the image and V is a trivializing neighborhood of $p_2(z)$ as above, then the connected component of $p_2^{-1}(V)$ containing z is disjoint from the image of p_Y, otherwise it would be contained in it (by the same argument as before), which is a contradiction. □

Proof of Proposition. By the Lemma, $Y \to Z$ is a cover. If $H = \mathrm{Aut}(Y|Z)$, we need to show that H acts transitively on the fibres of p_Y. Pick z in Z and let y_1, y_2 be two points in $p_Y^{-1}(z) \subset Y$. Then, there exists some φ in $\mathrm{Aut}(Y|X)$ such that $\varphi(y_1) = y_2$ because $Y \to X$ is Galois. Then, φ descends to an automorphism of Z if and only if φ lies in H, and

$$\varphi \in H \iff \{y \in Y : p_Y(y) = p_Y(\varphi(y))\} = Y,$$

which is true by Lemma 2.8 applied to p_Y and $p_Y \circ \varphi$. □

Corollary 2.17. The assignments $H \mapsto Y/H$ and $Z \mapsto \mathrm{Aut}(Y|Z)$ induce an inclusion-reversing bijection

$$\left\{ \text{ subgroups } H \leq \mathrm{Aut}(Y|X) \ \right\} \longleftrightarrow \left\{ \text{connected covers} \quad \begin{array}{ccc} Y & \longrightarrow & Z \\ & \searrow \quad \swarrow & \\ & X & \end{array} \right\}.$$

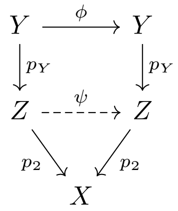
Proposition 2.18. In the above correspondence, the cover $Z \to X$ is Galois if and the subgroup $H \leq \mathrm{Aut}(Y|X)$ is normal, and in this case

$$\mathrm{Aut}(Z|X) \cong \mathrm{Aut}(Y|X)/H.$$

Proof. If H is normal in $G \coloneqq \mathrm{Aut}(Y|X)$, then $\frac{G}{H}$ acts on $\frac{Y}{H}$ and

$$\left(\frac{Y}{H}\right) / \left(\frac{G}{H}\right) \cong Y/G \cong X.$$

So, $Y/H \to X$ is Galois with group G/H. Suppose now that $Z \to X$ is Galois. We first show that if $\varphi \in \mathrm{Aut}(Y|X)$, then it induces an automorphism of $\mathrm{Aut}(Z|X)$. Indeed, take $y \in Y$ consider the diagram



Then, $x = (p_2 \circ p_Y)(y) \in X$ and $p_Y(y), p_Y(\varphi(y)) \in p_2^{-1}(x)$. Since $Z \to X$ is Galois, there exists a unique $\psi \in \mathrm{Aut}(Z|X)$ such that $\psi(p_Y(y)) = p_Y(\varphi(y))$ and we claim that this ψ makes the diagram commute, i.e. $\psi \circ p_Y = p_Y \circ \varphi$. However, the two maps agree on y and thus coincide on all of Y by Lemma 2.8. The assignment $\varphi \mapsto \psi$ then induces a homomorphism

$$\rho : \mathrm{Aut}(Y|X) \to \mathrm{Aut}(Z|X)$$

with kernel $\mathrm{Aut}(Y|Z)$, which is thus normal in $\mathrm{Aut}(Y|X)$. □

2.2 Monodromy and the Universal Cover

Suppose now X is locally path-connected.

Notation. For $x \in X$, we denote by $\pi_1(X, x)$ the fundamental group of X, that is the group of homotopy classes of loops based at x, where the group operation is given by concatenation of loops **with the convention that if f, g are loops then $f \bullet g$ is given by first going along g and then along f.** We denote by I the unit interval $[0, 1]$.

The following lemma is a standard result from the theory of of covers.

Lemma 2.19. If $Y \to X$ is a cover and $f : I \to X$ represents an element $\alpha \in \pi_1(X, x)$. If we take y in $p^{-1}(x)$, then f has a unique lifting $\tilde{f} : I \to Y$ such that $\tilde{f}(0) = y$. Moreover, if f_1 is another representative of α, then

$$\tilde{f}(1) = \tilde{f}_1(1).$$

Definition 2.20 (Monodromy action)**.** There is a left action of $\pi_1(X, x)$ on $p^{-1}(x)$ given

$$\alpha \cdot y := \tilde{f}(1),$$

where f is any representative of $\alpha \in \pi_1(X, x)$ and $\tilde{f}$ is the unique lifting of f such that $\tilde{f}(0) = y$.

Fix a base point x in X. We define a functor

$$\begin{aligned} \mathrm{Fib}_x \colon \{\text{covers of } X\} &\to \{\text{sets with a left } \pi_1(X, x)\text{-action}\} \\ (Y \xrightarrow{p} X) &\longmapsto p^{-1}(x), \end{aligned}$$

where the fibre $p^{-1}(x)$ above the base point is equipped with the monodromy action. To a morphism $f\colon Y \to Z$ of covers we associate the restriction $f|_{p_Y^{-1}(x)}\colon p_Y^{-1}(x) \to p_Z^{-1}(x)$, which is compatible with the action of $\pi_1(X,x)$. The main result of this section is the following:

Theorem 2.21. Let X be a connected and locally simply connected space, and take x in X. Then, the functor Fib_x induces an equivalence of categories

$$\{\text{ covers of } X \} \longleftrightarrow \{ \text{ left } \pi_1(X,x)\text{-sets } \}$$

where connected covers correspond to transitive $\pi_1(X,x)$-sets. Moreover, Galois covers correspond to coset spaces of normal subgroups of $\pi_1(X,x)$.

Definition 2.22. Let $\mathcal{C}$ be a category and let $F\colon \mathcal{C} \to \mathrm{Sets}$ be a functor. Then, F is *representable* if there exists an object $A \in \mathcal{C}$ such that

$$F \cong \mathrm{Hom}_{\mathcal{C}}(A, -)$$

as functors.

Note. Whenever it exists, such a representing object A is unique up to unique isomorphism.

Proposition 2.23. In the situation of the above theorem, the functor Fib_x is representable by a cover $\widetilde{X}_x \to X$, called the *universal cover* of X at x.

Remark 2.24. In particular, representability tells us that $\mathrm{Hom}(\widetilde{X}_x, \widetilde{X}_x) \cong \pi^{-1}(x)$, so there is some element $\tilde{x}$ in $\widetilde{X}_x$ which corresponds to $\mathrm{id}_{\widetilde{X}_x}$, and this "universal element" identifies a distinguished lift of x in any other cover $Y \to X$ via the unique morphism $\widetilde{X}_x \to Y$.

Proof. We first prove that Fib_x is representable by such a cover $\widetilde{X}_x \to X$ as a functor

$$\mathrm{Fib}_x\colon \{\text{spaces over } X\} \to \{\text{sets}\},$$

ignoring the monodromy action. We construct the cover $\widetilde{X}_x$ as follows: as a set, it is given by

$$\widetilde{X}_x := \{\text{homotopy classes of paths } I \xrightarrow{f} X, f(0) = x\}$$

with the map $\pi\colon \widetilde{X}_x \to X$ given by evaluating a path at 1.

For the topology, pick any $\tilde{y} \in \widetilde{X}_x$ represented by a path $f\colon I \to X$ and set $x = f(0), y = f(1)$. We then pick a simply connected open neighborhood U of y in X, and define a basis of open neighborhoods $\widetilde{U}_y$ of $\tilde{y}$ as the "continuations" of f to points inside U: since U is simply connected, the continuation only depends on the endpoint in U. This is a basis of open neighborhoods because if $\widetilde{U}_y$ and $\widetilde{V}_y$ are two such neighborhoods, then there exists a simply connected $W \subset U \cap V$ containing y, and $\widetilde{W}_y \subset \widetilde{U}_y \cap \widetilde{V}_y$.

This topology makes π continuous, and moreover π is a cover: indeed, for $\tilde{z} \in \widetilde{U}_y$ we have $\widetilde{U}_y = \widetilde{U}_z$,and if $\tilde{y}, \tilde{y}' \in \pi^{-1}(y)$ are distinct then $\widetilde{U}_y \neq \widetilde{U}_{y'}$ and thus $\widetilde{U}_y \cap \widetilde{U}_{y'} = \emptyset$. Therefore,

$$\pi^{-1}(U) = \bigsqcup_{\tilde{y} \in \pi^{-1}(y)} \widetilde{U}_y$$

Note. The "universal element" $\tilde{x} \in \pi^{-1}(x)$ is represented by the constant path $I \to \{x\}$.

Finally, we need to show that $\widetilde{X}_x$ represents Fib_x, that is given a cover $Y \xrightarrow{p} X$ we have a functorial bijection

$$y \in p^{-1}(x) \overset{1:1}{\longleftrightarrow} \pi_y \in \mathrm{Hom}_X(\widetilde{X}_x, Y)$$

Pick $y \in p^{-1}(x)$ and $\tilde{x}' \in \widetilde{X}_x$ represented by a path $I \xrightarrow{g} X$ with $g(0) = x$ and $g(1) = \pi(\tilde{x}')$. Then, g has a unique lifting $\tilde{g} \colon I \to Y$ such that $\tilde{g}(0) = y$, and we define

$$\pi_y(\tilde{x}') \coloneqq \tilde{g}(1).$$

It's easy to check that π_y is continuous and that $p \circ \pi_y = \pi$. The inverse is given by evaluating at the universal element $\tilde{x}$, and functoriality is straightforward. □

Remark 2.25. Consider now an automorphism $\varphi \in \mathrm{Aut}(\widetilde{X}_x|X)$. Given a cover $Y \xrightarrow{p} X$, precomposition by φ gives a bijection of $\mathrm{Hom}_X(\widetilde{X}_x, Y)$ with itself and thus also a bijection of $\mathrm{Fib}_x(Y)$:

$$\begin{array}{ccc} \mathrm{Hom}_X(\widetilde{X}_x, Y) & \xrightarrow{\cong} & \mathrm{Fib}_x(Y) \\ \downarrow \varphi^* & & \downarrow \\ \mathrm{Hom}_X(\widetilde{X}_x, Y) & \xrightarrow{\cong} & \mathrm{Fib}_x(Y) \end{array}$$

Therefore, the left action of $\mathrm{Aut}(\widetilde{X}_x|X)$ on $\widetilde{X}_x$ induces a right action on $\mathrm{Fib}_x(Y) \cong \mathrm{Hom}(\widetilde{X}_x, Y)$. However, we can turn it into a left action with the following trick:

Definition 2.26. If G is a group, the *opposite group* G^{op} is the group with the same underlying set as G, and with multiplication given by

$$(g, h) \mapsto h \cdot g.$$

Moreover, every right action of G on a set S corresponds to a left action of G^{op} on S via

$$g \cdot s \longleftrightarrow s \cdot g.$$

Proposition 2.27. $\widetilde{X}_x$ is a Galois cover of X, and there is a canonical isomorphism of groups

$$\mathrm{Aut}(\widetilde{X}_x|X) \cong \pi_1(X, x)^{\mathrm{op}}.$$

In this way, the action of $\mathrm{Aut}(\widetilde{X}_x|X)$ on $\mathrm{Fib}_x(Y)$ described above corresponds to the monodromy action of $\pi_1(X, x)$. This will follow from the construction of the isomorphism given below.

Lemma 2.28. The space $\widetilde{X}_x$ is path-connected.

Proof. We prove that the universal element $\tilde{x}$ can be connected to every other $\tilde{x}' \in \widetilde{X}_x$. Suppose $\tilde{x}'$ is represented by a path $I \xrightarrow{f} X$, and consider the composition with the multiplication map

$$\begin{aligned} I \times I &\to X \\ (s,t) &\mapsto f(st). \end{aligned}$$

For every fixed s, we get a map $f_s \colon I \to X$ such that f_0 is the constant path at x and $f_1 = f$. One then checks that

$$s \mapsto [f_s]$$

is a continuous map from I to $\widetilde{X}_x$, and so it defines a path joining $\tilde{x}$ to $\tilde{x}'$ which is the unique lifting of f to $\widetilde{X}_x$. □

Lemma 2.29. If X is simply connected and locally path-connected, every cover $Y \xrightarrow{p} X$ is trivial.

Proof. Assume without loss of generality that Y is connected. Then, by assumption it must also be path-connected. Pick $y_0, y_1 \in Y$ and suppose that $x = p(y_0) = p(y_1)$. We want to show that $y_0 = y_1$. Since Y is path-connected, there exists a path $I \xrightarrow{\tilde{f}} Y$ such that $\tilde{f}(0) = y_0$ and $\tilde{f}(1) = y_1$. Then, $f := p \circ \tilde{f}$ is a closed path in X around x, but X is simply connected and so f is homotopic to the constant path $I \xrightarrow{c} \{x\}$. The unique lifting $\tilde{c}$ of c such that $\tilde{c}(0) = y_0$ is the constant path at y_0, so by uniqueness of the lifting we get $y_1 = \tilde{f}(1) = \tilde{c}(1) = y_0$. □

Corollary 2.30. Let X be a locally simply connected space. If $Y \xrightarrow{p} X$ is a cover of X and $Z \xrightarrow{q} Y$ is a cover of Y, then $q \circ p : Z \to X$ is a cover of X.

Proof. If U is a simply connected neighborhood of X, then $p^{-1}(U)$ is a disjoint union of simply connected open sets U_i homeomorphic to U, but then $q^{-1}(U_i)$ is a disjoint union of open sets homeomorphic to U_i (by the above lemma, as U_i is simply connected), and thus $q{\circ}p$ is a cover. □

Proof of Proposition 2.27. We want to show that $\widetilde{X}_x \to X$ is a Galois cover. By Lemma 2.28, we know it is connected, so we only need to show that $\mathrm{Aut}(\widetilde{X}_x|X)$ acts transitively on **one** fibre, namely on $\pi^{-1}(x)$. Pick $\tilde{y} \in \pi^{-1}(x)$ which corresponds by representability to a morphism of covers $\pi_{\tilde{y}} \colon \widetilde{X}_x \to \widetilde{X}_x$ with $\pi_{\tilde{y}}(\tilde{x}) = \tilde{y}$. We claim that $\pi_{\tilde{y}}$ is an automorphism of covers. We have already seen (Lemma 2.30) that π_y is a connected cover, in particular it is surjective. Take some $\tilde{z} \in \pi_{\tilde{y}}^{-1}(\tilde{x})$. Again, by representability it gives a morphism of covers $\pi_{\tilde{z}} \colon \widetilde{X}_x \to \widetilde{X}_x$ such that $\pi_{\tilde{z}}(\tilde{x}) = \tilde{z}$. In particular, $\pi_{\tilde{y}} \circ \pi_{\tilde{z}}(\tilde{x}) = \tilde{x}$, so Lemma 2.8 implies

$$\pi_{\tilde{y}} \circ \pi_{\tilde{z}} = \mathrm{id}_{\widetilde{X}_x},$$

but since these are surjective maps this shows injectivity of $\pi_{\tilde{y}}$, which concludes.

We now move on to the isomorphism between $\pi_1(X,x)^{\mathrm{op}}$ and $\mathrm{Aut}(\widetilde{X}_x|X)$. Recall that there is a right action of $\pi_1(X,x)$ on $\widetilde{X}_x$. If $\tilde{x}' \in \widetilde{X}_x$ is represented by $f\colon I \to X$ with $f(0) = x$ and $\alpha \in \pi_1(X,x)$ is represented by f_α such that $f_\alpha(0) = f_\alpha(1) = x$, then the corresponding left action of $\pi_1(X,x)^{\mathrm{op}}$ on $\widetilde{X}_x$ is given by concatenation:

$$\alpha \cdot \tilde{x}' \coloneqq [f \bullet f_\alpha].$$

This defines a map

$$\begin{aligned} \pi_1(X,x)^{\mathrm{op}} &\to \mathrm{Aut}(\widetilde{X}_x|X) \\ \alpha &\mapsto \varphi_\alpha \coloneqq (\tilde{x}' \mapsto \alpha \cdot \tilde{x}'). \end{aligned}$$

This is a homomorphism, and it is injective because if $\alpha \neq 1$ then it moves $\tilde{x}$. For surjectivity, given $\varphi \in \mathrm{Aut}(\widetilde{X}_x|X)$ we need to show that it comes from some $\alpha \in \pi_1(X,x)$. Consider $\tilde{x}' = [f] \in \widetilde{X}_x$ and its image $\varphi(\tilde{x}') = [g]$. Here g is a path starting from x and ending at $f(1)$. Denote by α the class of $f^{-1} \bullet g$ in $\pi_1(X,x)$. The associated ϕ_α coincides with ϕ in $\tilde{x}'$, so they are equal by the usual lemma. □

Propositions 2.23 and 2.27 together imply Theorem 2.21, in the same way as in Grothendieck's form of Galois theory (Theorem 1.35).

Remark. In general, consider a category $\mathcal{C}$ and a functor $F\colon \mathcal{C} \to \mathrm{Sets}$ representable by some object A. Then, there is an isomorphism

$$\mathrm{Aut}(F) \cong \mathrm{Aut}(A)^{\mathrm{op}},$$

where $\mathrm{Aut}(F)$ is the group of automorphisms of the functor F.

In view of the above fact, we can define the fundamental group of any topological space X as

$$\pi_1(X,x) = \mathrm{Aut}(\mathrm{Fib}_x).$$

Complements.

- The universal cover $\widetilde{X}_x$ is simply connected. There are at least 2 ways to see this:
    1. directly, from the explicit construction of $\widetilde{X}_x$;
    2. showing that the cover $\widetilde{X}_x \xrightarrow{\mathrm{id}} \widetilde{X}_x$ represents the fibre functor $\mathrm{Fib}_{\tilde{x}}$ on the category of covers of $\widetilde{X}_x$, where $\tilde{x}$ is the universal element.
- If we pick some $x' \in X$ and choose a path f from x' to x, this induces by precomposition a map $\widetilde{X}_x \xrightarrow{\varphi_f} \widetilde{X}_{x'}$, which is a homeomorphism. This in turn induces an inner automorphism

  $$\begin{aligned} \mathrm{Aut}(\widetilde{X}_x|X) &\to \mathrm{Aut}(\widetilde{X}_{x'}|X) \\ \varphi &\mapsto \varphi_f^{-1} \circ \varphi \circ \varphi_f, \end{aligned}$$

  and thus an isomorphism $\pi_1(X,x)^{\mathrm{op}} \to \pi_1(X,x')^{\mathrm{op}}$. One checks that this coincides with the usual isomorphism between fundamental groups based at different points, in particular it depends on the choice of the path f.

2.3 Finite covers

Definition 2.31. A cover $Y \to X$ is *finite* if all of its fibres are finite.

Let X be a connected and locally simply connected space, and fix a base point x in X. By considering the profinite completion $\widehat{\pi_1(X,x)}$ of $\pi_1(X,x)$, we get an analogue of Theorem 2.21 for finite covers:

Corollary 2.32. The functor Fib_x induces an equivalence of categories

$$\{\text{finite covers of } X\} \longleftrightarrow \{\text{finite continuous left } \widehat{\pi_1(X,x)}\text{-sets}\}.$$

Proof. If $Y \to X$ is a finite cover, then $\pi_1(X,x)$ acts on $\mathrm{Fib}_x(Y)$ via a finite quotient, and so $\widehat{\pi_1(X,x)}$ acts on $\mathrm{Fib}_x(Y)$ as well. The stabilizer of any point y in $\mathrm{Fib}_x(Y)$ has finite index in $\pi_1(X,x)$, so it contains a normal subgroup V of finite index. But then, $\pi_1(X,x)/V$ is one of the finite quotients of $\widehat{\pi_1(X,x)}$, and if we take $\widehat{V}$ to be the open subgroup $\ker(\widehat{\pi_1(X,x)} \to \pi_1(X,x)/V)$ then the stabilizer of y in $\widehat{\pi_1(X,x)}$ is a union of finitely many cosets of $\widehat{V}$, and is thus open.

Conversely, if S is a finite continuous $\widehat{\pi_1(X,x)}$-set, then it becomes a finite $\pi_1(X,x)$-set via the natural map

$$\pi_1(X,x) \to \widehat{\pi_1(X,x)},$$

and therefore gives a finite cover. □

From now on, let X be a locally connected space. We start by recalling some facts about finite covers.

Remark 2.33. If $Y \xrightarrow{p} X$ and $Z \xrightarrow{q} Y$ are finite covers, then the finitness allows us to deduce that the composite $q \circ p \colon Z \to X$ is always a finite cover (compare with Corollary 2.30). The verification is an easy exercise.

Definition 2.34. If $Y_1 \xrightarrow{p_1} X$ and $Y_2 \xrightarrow{p_2} X$ are two spaces over X, their *fibre product* is the space

$$Y_1 \times_X Y_2 \coloneqq \{(y_1, y_2) \in Y_1 \times Y_2 \colon p_1(y_1) = p_2(y_2)\}$$

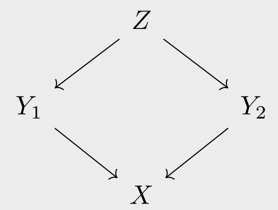
which comes with natural projections fitting into the commutative diagram

$$\begin{array}{ccc} Y_1 \times_X Y_2 & \xrightarrow{q_2} & Y_2 \\ \downarrow{\scriptstyle q_1} & & \downarrow{\scriptstyle p_2} \\ Y_1 & \xrightarrow{p_1} & X \end{array}$$

Remark 2.35. If $Y_1 \xrightarrow{p_1} X$ is a cover, then the projection $q_2 \colon Y_1 \times_X Y_2 \to Y_2$ is also a cover. (Proof easy.)

Corollary 2.36.

1. If $Y_1 \xrightarrow{p_1} X$ and $Y_2 \xrightarrow{p_2} X$ are finite covers, then the fibre product $Y_1 \times_X Y_2 \to X$ is a finite cover as well.
2. If $Y_1 \to X$ and $Y_2 \to X$ are finite connected covers, then there exists a finite connected cover $Z \to X$ making the following diagram commute:



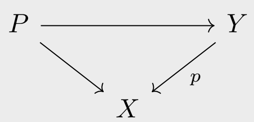
(it's enough to take a connected component of $Y_1 \times_X Y_2 \to X$.)

Remark 2.37. Let $Y \to X$ be a finite cover. Then, the diagonal

$$\Delta(Y) \coloneqq \{(y, y) \in Y \times_X Y\} \subset Y \times_X Y$$

is open and closed. Indeed, if $(y, y) \in \Delta(Y)$, then there exists a small enough open neighborhood U of y such that $U \times U \subset \Delta(Y)$, so $\Delta(Y)$ is open. Moreover, if $(y_1, y_2) \in (Y \times_X Y)$ with $y_1 \neq y_2$, then there exists a neighborhood U of $p(y_1) = p(y_2)$ such that $p^{-1}(U) = \bigsqcup_{i=1}^n U_i$ and $y_1 \in U_i$ and $y_2 \in U_j$ for some $i \neq j$. But then, $(U_1 \times U_2) \cap \Delta(Y) = \emptyset$, so $\Delta(Y)$ is also closed.

Proposition 2.38. If $Y \to X$ is a finite connected cover, then there exists a finite Galois cover $P \to X$ which factors through Y, that is



Proof (Serre). Fix $x \in X$ and let $p^{-1}(x) = \{y_1, \dots, y_n\}$. The n-fold fibre product

$$Y^n \coloneqq Y \times_X Y \times_X \cdots \times_X Y$$

is a finite cover of X by a previous corollary. Now fix $\overline{y} = (y_1, \dots, y_n) \in Y^n$ and let P be the connected component of $\overline{y}$. Define a map $P \to Y$ by restriction of the first projection $Y^n \to Y$ to P; its composition with p is the restriction of the natural map $Y^n \to X$ to P.

We claim that $P \to X$ is Galois. First observe that every point of $\pi^{-1}(x)$ is of the form

$$(y_{\sigma(1)}, \dots, y_{\sigma(n)})$$

for some $\sigma \in S_n$: indeed, suppose there is an element of the form $(y, y, \star, \dots, \star) \in \pi^{-1}(x)$, and denote by $p_{12} \colon Y^n \to Y \times_X Y$ the projection to the first 2 components. Then, $\pi^{-1}(x) \cap p_{12}^{-1}(\Delta(Y))$

is nonempty, but $p_{12}^{-1}(\Delta(Y))$ is open and closed in Y^n by the above remark and $P \cap p_{12}^{-1}(\Delta(Y)) \neq \emptyset$, so $P \subset p_{12}^{-1}(\Delta(Y))$ which is a contradiction, because $\overline{y} \in P$. This shows that the first two entries in an element of $\pi^{-1}(x)$ must be different, and a similar argument works for any two entries.

Therefore, suppose that $\overline{y}_\sigma \coloneqq (y_{\sigma(1)}, \ldots, y_{\sigma(n)}) \in \pi^{-1}(x)$, and make σ act on Y^n by permutation of the factors. Then, φ_σ is an automorphism of Y^n over X, and

$$\varphi_\sigma(\overline{y}) = \overline{y}_\sigma \implies \varphi_\sigma(P) \cap P \neq \emptyset,$$

so $\varphi_\sigma(P) = P$ because P is a connected component. This shows that S_n acts on P and transitively on $\pi^{-1}(x)$, so $P \to X$ is Galois. □

Construction 2.39 (Grothendieck)**.** Fix a space (X, x) with a basepoint, and consider the set

$$\{(P_\alpha, p_\alpha) \mid P_\alpha \xrightarrow{\pi_\alpha} X \text{ is a finite Galois cover with a fixed element } p_\alpha \in \pi_\alpha^{-1}(x)\}.$$

This has a partial order given by $(P_\alpha, p_\alpha) \leq (P_\beta, p_\beta)$ if and only if there exists a morphism of covers $\varphi_{\alpha\beta} \colon P_\beta \to P_\alpha$ which sends p_α to p_β.

Note. If $(P_\alpha, p_\alpha) \leq (P_\beta, p_\beta)$, then the map $\varphi_{\alpha\beta}$ is unique.

This is a directed poset: indeed, by Corollary 2.36 (2), given (P_α, p_α) and (P_β, p_β) there is a finite connected cover Z which dominates both, and by the previous proposition there exists a finite Galois cover P_γ which dominates Z, and thus also P_α and P_β. Since P_γ is Galois, by composing with suitable automorphisms we can arrange that p_γ is mapped to p_α and p_β.

At this point, we can define $\widehat{X}_x$ as the inverse limit

$$\widehat{X}_x \coloneqq \varprojlim P_\alpha,$$

which comes with a natural map $\widehat{X}_x \xrightarrow{\pi} X$ and a universal element $p_x \coloneqq (p_\alpha)_\alpha \in \pi^{-1}(x)$.

Definition 2.40. Let $(\Lambda, \leq)$ be a directed poset. A direct system of sets indexed by Λ is given by sets S_α for every $\alpha \in \Lambda$ and transition maps $\varphi_{\alpha\beta} \colon S_\alpha \to S_\beta$ for every $\alpha \leq \beta$ such that $\varphi_{\alpha\alpha} = \mathrm{id}_{S_\alpha}$ and $\varphi_{\beta\gamma} \circ \varphi_{\alpha\beta} = \varphi_{\alpha\gamma}$ for every $\alpha \leq \beta \leq \gamma$. The direct limit of such a system is the set

$$\varinjlim S_\alpha \coloneqq \bigsqcup_{\alpha \in \Lambda} S_\alpha / \sim,$$

where $\sim$ is the equivalence relation defined by $s_\alpha \sim s_\beta$ if and only if there exists $\gamma \geq \alpha, \beta$ such that $\varphi_{\alpha\gamma}(s_\alpha) = \varphi_{\beta\gamma}(s_\beta)$.

Let now $Y \to X$ be a finite cover. Then, since $(P_\alpha)_\alpha$ is an inverse system, the sets $\mathrm{Hom}_X(P_\alpha, Y)$ form a direct system, and we can define the direct limit

$$\mathrm{Hom}^{\mathrm{pro}}(\widehat{X}_x, Y) \coloneqq \varinjlim \mathrm{Hom}_X(P_\alpha, Y).$$

Theorem 2.41. For every finite cover $Y \xrightarrow{p} X$, there is a canonical bijection

$$p^{-1}(x) \overset{1:1}{\longleftrightarrow} \mathrm{Hom}^{\mathrm{pro}}(\widehat{X}_x, Y)$$

which is functorial in Y.

Proof. If $\varphi\colon \widehat{X}_x \dashrightarrow Y$ is an element in $\mathrm{Hom}^{\mathrm{pro}}(\widehat{X}_x, Y)$ then $\varphi(p_x) = y \in Y$ lies in the fiber $p^{-1}(x)$. Indeed, φ is represented by some morphism of covers $P_\alpha \to Y$ sending p_α to y, and since $p_\alpha \in \pi_\alpha^{-1}(x)$ we have $y \in p^{-1}(x)$.

Conversely, assume that $Y \to X$ is connected and take some $y \in p^{-1}(x)$. Then, by correspondence there exists a finite Galois cover $P_\alpha \to X$ dominating Y which sends p_α to y. By construction, this defines an element φ_y in $\mathrm{Hom}^{\mathrm{pro}}(\widehat{X}_x, Y)$ such that $\varphi_y(p_x) = y$. ☐

Definition 2.42. If $Y \xrightarrow{p} X$ is a finite cover, the profinite group

$$\widehat{\pi}_1(X, x) \coloneqq \varprojlim \underbrace{\mathrm{Aut}(P_\alpha|X)^{\mathrm{op}}}_{\text{finite}}$$

acts functorially on each finite cover and thus on $\widehat{X}_x$, so it acts on $p^{-1}(x)$ via Theorem 2.41.

In this way, we get an equivalence of categories

$$\{\text{finite covers of } X\} \longleftrightarrow \{\text{finite continuous left } \widehat{\pi}_1(X, x)\text{-sets}\}.$$

We conclude this section with a recent result by Kucharczyk and Scholze [3] from 2018:

Theorem 2.43. Let K be a field of characteristic 0 containing all roots of unity (i.e. $K \supset \mathbb{Q}(\mu_\infty)$). Then, there exists a compact Hausdorff space X_K such that

$$\widehat{\pi}_1(X_K) \cong \mathrm{Gal}(\overline{K}|K).$$

Caveat. The space X_K constructed in [3] is not locally connected, so one needs to generalize the above construction by modifying the proofs of some of the lemmas.

Construction 2.44. Put the discrete topology on $\overline{K}^\times$, and consider its *Pontryagin dual*

$$(\overline{K}^\times)^\vee \coloneqq \mathrm{Hom}_{\mathrm{cont}}(\overline{K}^\times, S^1).$$

This is naturally endowed with the compact-open topology, whose sub-basis is given by sets of the form

$$V(K, U) = \{\chi\colon \overline{K}^\times \to S^1 \mid \chi(K) \subset U\}$$

with K compact and U open. Similarly, we define

$$X_{\overline{K}} \coloneqq (\overline{K}^\times/\mu_\infty)^\vee$$

which comes with a natural left action of $G_K = \mathrm{Gal}(\overline{K}|K)$:

$$\sigma \cdot \chi(x) \coloneqq \chi(\sigma^{-1}(x)).$$

Finally, the desired space is obtained as the quotient of $X_{\overline{K}}$ by this action:

$$X_K \coloneqq X_{\overline{K}}/G_K.$$

2.4 Sheaf theory

Let X be a topological space, and consider the category $\mathcal{C}_X$ whose objects are nonempty open subsets $U \subset X$ whose morphisms between V and U are

$$\mathrm{Hom}_{\mathcal{C}_X}(V, U) = \begin{cases} \{i \colon V \hookrightarrow U\} & \text{if } V \subset U, \\ \emptyset & \text{otherwise.} \end{cases}$$

Definition 2.45. A *presheaf* of sets on X is a contravariant functor

$$\mathcal{F} \colon \mathcal{C}_X \to \mathrm{Sets}.$$

(similarly, one defines presheaves of groups, modules, etc. by landing in the appropriate category.)

Concretely, a presheaf assigns to every open $U \subset X$ a set $\mathcal{F}(U)$, and to each inclusion $V \subset U$ a map $\mathcal{F}(U) \to \mathcal{F}(V)$ often called the restriction map. The following example shows why.

Example 2.46. A basic example to keep in mind is the presheaf of continuous functions

$$U \mapsto C^0(U, \mathbb{R}),$$

with the usual restriction of functions.

Definition 2.47. A presheaf $\mathcal{F}$ is a *sheaf* if

- for every open covering $\{U_i \colon i \in I\}$ of U and for every $f, g \in \mathcal{F}(U)$ such that $f|_{U_i} = g|_{U_i}$ for all $i \in I$, then $f = g$, and
- for every open covering $\{U_i \colon i \in I\}$ of U and for every family of elements $f_i \in \mathcal{F}(U_i)$ such that $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ for all $i, j \in I$, there exists some $f \in \mathcal{F}(U)$ such that $f|_{U_i} = f_i$ for all $i \in I$.

We can state the above definition more concisely via the exactness of the following sequence of sets:

$$\begin{array}{ccccc} \mathcal{F}(U) & \hookrightarrow & \prod_{i \in I} \mathcal{F}(U_i) & \rightrightarrows & \prod_{(i,j) \in I^2} \mathcal{F}(U_i \cap U_j) \\ f & \longmapsto & (f|_{U_i})_{i \in I} & \longmapsto & (f|_{U_i \cap U_j})_{(i,j) \in I^2} \end{array}$$

Example 2.48.

- If X is a smooth (resp. complex) manifold, sending an open $U \subset X$ to all C^∞ functions from $U \to \mathbf{R}$ (resp. holomorphic functions $U \to \mathbf{C}$) defines a sheaf.
- If X and A are topological spaces, there is a sheaf

  $$\mathcal{F}(U) = \{\text{continuous functions } U \to A\}.$$

  In the special case where A is discrete, this is the *constant sheaf* with values in A (note that for $U \subset X$ connected $\mathcal{F}(U) = A$).

Remark 2.49. The collection of (pre)sheaves on X forms a category: a morphism $\mathcal{F} \xrightarrow{\varphi} \mathcal{G}$ between (pre)sheaves is a morphism of functors $\mathcal{C}_X \to \text{Sets}$. Concretely, it assigns to each nonempty open set a function

$$\mathcal{F}(U) \xrightarrow{\varphi_U} \mathcal{G}(U)$$

such that for $V \subset U$ the diagram

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\varphi_U} & \mathcal{G}(U) \\ \downarrow & & \downarrow \\ \mathcal{F}(V) & \xrightarrow{\varphi_V} & \mathcal{G}(V) \end{array}$$

commutes, where the vertical maps are the restriction maps. An isomorphism of sheaves is given by an isomorphism of functors.

Definition 2.50. A sheaf $\mathcal{F}$ is *locally constant* if there exists an open covering $\{U_i : i \in I\}$ such that for all i the sheaf $\mathcal{F}|_{U_i}$ is isomorphic to a constant sheaf in the category of sheaves on U_i.

Construction 2.51. Let $Y \xrightarrow{p} X$ be a space over X. A *section* of p over an open subset $U \subset X$ is a continuous map $s\colon U \to Y$ such that $p \circ s = \mathrm{id}_U$:

$$\begin{array}{ccc} Y & \xrightarrow{p} & X \\ & \nwarrow^{s} & \uparrow \\ & & U \end{array}$$

Define a presheaf $\mathcal{F}_Y$ on X by

$$\mathcal{F}_Y(U) := \{\text{sections } U \to Y \text{ of } p \text{ over } U\},$$

with the natural restriction maps $\mathcal{F}_Y(U) \to \mathcal{F}_Y(V)$ for $V \subset U$; note that this is in fact a sheaf, as sections can be glued together.

Assume from now on that X is locally connected.

Lemma 2.52. If $Y \xrightarrow{p} X$ is a cover, then $\mathcal{F}_Y$ is a locally constant sheaf of sets, and when X is connected it is constant if and only if Y is a trivial cover.

Proof. If $U \subset X$ is a connected open such that $p^{-1}(U) \cong U \times F$ for some discrete set F and $s\colon U \to Y$ is a section, then $s(U) \subset Y$ is a connected open which is homeomorphic to U via p. Therefore, $s(U)$ is of the form $U \times \{f\}$ for some $f \in F$, and so sections over U correspond to elements of F. $\square$

We now describe a correspondence between sheaves and certain spaces over X.

Construction 2.53. Let $\mathcal{F}$ be a presheaf (of sets) on X. We want to construct a space $X_{\mathcal{F}}$ over X.

Definition 2.54. The *stalk* of $\mathcal{F}$ at a point $x \in X$ is the set

$$\mathcal{F}_x \coloneqq \varinjlim_{U \ni x} \mathcal{F}(U),$$

where the limit is taken over all open neighborhoods of x ordered by reverse inclusion: $U \leq V$ if and only if $V \subset U$. Explicitly, an element of $\mathcal{F}_x$ is represented by some $f \in \mathcal{F}(U)$, with two elements $f_1 \in \mathcal{F}(U_1)$ and $f_2 \in \mathcal{F}(U_2)$ equivalent if there exists some open $V \subset U_1 \cap U_2$ with $f_1|_V = f_2|_V$.

We define a space over X by

$$X_{\mathcal{F}} \coloneqq \bigsqcup_{x \in X} \mathcal{F}_x$$

together with the projection map $p_{\mathcal{F}} \colon X_{\mathcal{F}} \to X$ sending $\mathcal{F}_x$ to x. To define a topology on $X_{\mathcal{F}}$, consider $U \subset X$ and associate to an element $s \in \mathcal{F}(U)$ the map

$$\begin{aligned} i_s \colon U &\to X_{\mathcal{F}} \\ x &\mapsto \text{ image of } s \text{ in } \mathcal{F}_x. \end{aligned}$$

Then, we endow $X_{\mathcal{F}}$ with the coarsest topology in which $i_s(U)$ is open for all open subsets $U \subset X$ and $s \in \mathcal{F}(U)$; one checks that $p_{\mathcal{F}}$ is continuous for this topology.

Note. If $\mathcal{F}$ is locally constant, then $p_{\mathcal{F}}$ is a cover. This is because on a connected open U where $\mathcal{F}$ is the constant sheaf given by a set F, we have $\mathcal{F}_x = F$ for all $x \in U$, and so

$$p_{\mathcal{F}}^{-1}(U) \cong U \times F.$$

Note. If $\mathcal{F} \to \mathcal{G}$ is a morphism of presheaves, then there is an induced map of spaces over X

$$X_{\mathcal{F}} \to X_{\mathcal{G}},$$

as for $x \in X$ there is an induced map $\mathcal{F}_x \to \mathcal{G}_x$ on stalks, and one checks that it is continuous.

Therefore, we have constructed a functor $\mathcal{F} \mapsto X_{\mathcal{F}}$ from the category of presheaves (of sets) on X to the category of spaces over X.

Theorem 2.55. The functor $\mathcal{F} \mapsto X_{\mathcal{F}}$ restricts to an equivalence of categories

$$\{ \text{ sheaves } \mathcal{F} \text{ on } X \ \} \longleftrightarrow \{ \text{ spaces } Y \xrightarrow{p} X \text{ over } X \colon p \text{ is a local homeomorphism}\},$$

with quasi-inverse $Y \mapsto \mathcal{F}_Y$. Moreover, this equivalence induces a correspondence

$$\{ \text{ locally constant sheaves on } X \ \} \longleftrightarrow \{ \text{ covers of } X \ \}.$$

Proof. We only deal with the case of locally constant sheaves, which is the one we will be interested in. Let $\mathcal{F}$ be a locally constant sheaf on X, and consider the locally constant sheaf $\mathcal{F}_{X_{\mathcal{F}}}$. We define a morphism of sheaves $\mathcal{F} \to \mathcal{F}_{X_{\mathcal{F}}}$ on some open $U \subset X$ by sending $s \in \mathcal{F}(U)$ to the section $i_s \colon U \to X_{\mathcal{F}}$.

Conversely, let $Y \xrightarrow{p} X$ be a cover, and consider the space $X_{\mathcal{F}_Y}$. This comes with the projection map $X_{\mathcal{F}_Y} \xrightarrow{p_{\mathcal{F}_Y}} X$. We define a map $Y \to X_{\mathcal{F}_Y}$ on each fibre $F := p^{-1}(x)$ as the identity, since $p_{\mathcal{F}_Y}^{-1}(x) = (\mathcal{F}_Y)_x \cong F$ because $Y \to X$ is a cover.

We have to check that $\mathcal{F} \mapsto \mathcal{F}_{X_\mathcal{F}}$ and $Y \mapsto X_{\mathcal{F}_Y}$ are functorial isomorphisms: it's enough to check this over elements of an open covering of X, and moreover we can take an open covering by connected opens on which $\mathcal{F}$ is constant (respectively, $Y \to X$ is trivial). But then, if $\mathcal{F}$ is the constant sheaf with value F, by Lemma 2.52 $Y = X \times F$, and we are done. □

Combining this with Theorem 2.21, we get the following result:

Theorem 2.56. Let X be a connected and locally simply connected space, and fix a point $x \in X$. The functor $\mathcal{F} \mapsto \mathcal{F}_x$ induces an equivalence of categories

$$\{\text{locally constant sheaves on } X\} \longleftrightarrow \{\text{left } \pi_1(X,x)\text{-sets}\}.$$

Remark 2.57. Sheaves were invented by the French mathematician Jean Leray. He in fact defined them via the spaces $X_\mathcal{F}$ constructed above. Today $X_\mathcal{F}$ is usually called the *espace étalé* associated with the sheaf $\mathcal{F}$. Note that if we take a presheaf $\mathcal{F}$ which is not a sheaf, then we can associate to it the sheaf $\mathcal{F}_{X_\mathcal{F}}$, which is called the *sheafification* of $\mathcal{F}$. It comes with a morphism of presheaves $\mathcal{F} \to \mathcal{F}_{X_\mathcal{F}}$ defined as above which is universal for presheaf morphisms of $\mathcal{F}$ in sheaves.

Recall that for a commutative ring R and a group G, the group algebra $R[G]$ is the free R-module with basis G, with multiplication induced by the group law on G.

Corollary 2.58. The rule $\mathcal{F} \mapsto \mathcal{F}_x$ induces an equivalence of categories

$$\{ \text{ locally constant sheaves of } R\text{-modules on } X \ \} \longleftrightarrow \{ \text{ left } R[\pi_1(X,x)]\text{-modules } \}.$$

Proof. If $\mathcal{F}$ is a locally constant sheaf of R-modules on X, then $\mathcal{F}_x$ is an R-module endowed (**as a set**) with an action of $\pi_1(X,x)$. Since the addition on $\mathcal{F}(U)$ is induced by the morphism of sheaves $\mathcal{F} \times \mathcal{F} \to \mathcal{F}$ given on $U \subset X$ by

$$\begin{aligned} \mathcal{F}(U) \times \mathcal{F}(U) &\to \mathcal{F}(U) \\ (s,t) &\mapsto s+t, \end{aligned}$$

the induced map $\mathcal{F}_x \times \mathcal{F}_x \to \mathcal{F}_x$ on stalks is also $(s_x, t_x) \mapsto (s+t)_x$, which is a morphism of $\pi_1(X,x)$-sets by functoriality. The same goes for scalar multiplication by $r \in R$, so we get an $R[\pi_1(X,x)]$-module structure on $\mathcal{F}_x$. □

Definition 2.59. A *complex local system* is a locally constant sheaf of finite-dimensional $\mathbf{C}$-vector spaces.

With this definition in hand, we deduce the following special case of the previous corollary:

Corollary 2.60. There is a correspondence

$$\{\text{complex local systems on } X\} \leftrightarrow \{\text{finite-dimensional complex representations of } \pi_1(X,x)\}$$

Example 2.61. Let $D \subset \mathbf{C}$ be a connected open set, and consider a homogeneous nth-order linear differential equation

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y' + a_0y = 0 \tag{2.1}$$

with the a_i holomorphic functions on D. Let $U \subset D$ be an open set. Local holomorphic solutions of (2.1) on U form a $\mathbf{C}$-vector space $\mathcal{S}(U)$, and by a famous theorem of Cauchy for sufficiently small U this is an n-dimensional space. Moreover, restricting elements of a basis to $V \subset U$ still gives a basis, so the $\mathcal{S}(U)$ form an n-dimensional local system. Moreover, it is a subsheaf of the sheaf $\mathcal{O}$ of holomorphic functions on D.

If we fix a base point $x \in D$, we can consider the *monodromy representation*

$$\pi_1(D,x) \to \mathrm{GL}_n(\mathbf{C})$$

associated with $\mathcal{S}$ via the above equivalence of categories. Concretely, it is given as follows. Take a loop $\gamma \in \pi_1(D,x)$ which is represented by a closed path $I \xrightarrow{f} D$ with $f(0) = f(1) = x$. To the sheaf $\mathcal{S}$, we have associated a cover $X_{\mathcal{S}} \to D$, and if we fix an element $s \in \mathcal{S}_x$ (i.e. a germ of a solution at x), it corresponds to a point of $X_{\mathcal{S}}$ in the fibre above x that we denote in the same way. Now there exists a unique lifting $\tilde{f}\colon I \to X_{\mathcal{S}}$ of f with $\tilde{f}(0) = s$ and the monodromy action is given by $\gamma \cdot s = \tilde{f}(1) \in \mathcal{S}_x$. This is the *analytic continuation of the local solution s along the path γ*. It exists and is unique (and depends only on the homotopy class of the path) because we are working with a locally constant sheaf of holomorphic functions. This is the origin of the theory of the fundamental group developed by Poincaré.

Example 2.62. Let us consider the simplest nontrivial case. The punctured unit disk

$$D = \{|z| < 1\} \setminus \{0\},$$

has fundamental group isomorphic to $\mathbf{Z}$. For any holomorphic function f on D which extends meromorphically to 0 (e.g. $f = \frac{1}{z}$), consider the differential equation

$$y' = fy. \tag{2.2}$$

We want to compute its monodromy representation

$$\mathbf{Z} \to \mathrm{GL}_1(\mathbf{C}) = \mathbf{C}^\times, \quad 1 \mapsto m$$

and we know that over simply connected open subsets solutions of (2.2) are of the form $\exp \circ F$, where F is a primitive of f which is determined up to translation by a constant. If we denote by U_+ and U_- the simply connected open subsets of D given by

$$U_+ = D \setminus (0,i), \quad U_- = D \setminus (0,-i),$$

whose intersection is

$$U_+ \cap U_- = C_+ \sqcup C_- = \{z \in D \mid \Re(z) > 0\} \sqcup \{z \in D \mid \Re(z) < 0\},$$

we can pick primitives F_+ and F_- of f on U_+ and U_- respectively such that they agree on C_-. This way, we can switch from F_- to F_+ as we go along a counterclockwise loop γ in D, and the monodromy is given by

$$m = \frac{\exp(F_-(x))}{\exp(F_+(x))} = \exp(F_-(x) - F_-(-x) + F_+(-x) - F_+(x)) = \exp\left(\int_\gamma f\right) = \exp(2\pi i \operatorname{Res}_0(f)).$$

For $f = \frac{1}{z}$, this residue is 1 and the monodromy is just $2\pi i$.

Example 2.63. Let $f\colon X \to Y$ be a smooth map between smooth manifolds X and Y, and let A be a constant sheaf on X associated with a ring A (e.g. $A = \mathbf{C}$). We define a sheaf $R^i f_* A$ on Y as the sheafification of the presheaf

$$U \mapsto H^i(f^{-1}(U), A),$$

so that the stalks are $(R^i f_* A)_y = H^i(f^{-1}(y), A)$. Assume now that f is proper (i.e. the inverse image of compact sets is compact), and that f is a submersion (i.e. its differential is surjective). Under these assumptions, $R^i f_* A$ is a locally constant sheaf of finitely generated A-modules. So, for $A = \mathbf{C}$ we get a complex local system. This is a consequence of Ehresmann's fibration theorem from differential topology, which asserts that f is a locally trivial fibration.

3 Riemann Surfaces

Let X be an Hausdorff topological space. A (1-dimensional) *complex atlas* on X is the datum of

- an open covering $\mathcal{U} = \{U_i : i \in I\}$ of X;
- for each $i \in I$ a map (called *chart*)

  $$f_i\colon U_i \to \mathbf{C}$$

  which is a homeomorphism onto its image, such that
- for every $i, j \in I$ the *transition map*

  $$f_i \circ f_j^{-1}\colon f_j(U_i \cap U_j) \to f_i(U_i \cap U_j)$$

  is holomorphic.

Two such atlases are equivalent if their union is still an atlas.

Definition 3.1. a *Riemann surface* is an Hausdorff topological space X together with an equivalence class of complex atlases.

Example 3.2.

1. If $U \subset \mathbf{C}$ is an open subset, then U with is a Riemann surface by taking the atlas with only one chart (U, id_U).

2. The Riemann sphere $\mathbb{P}^1_{\mathbf{C}}$, which as a topological space is just S^2, is a Riemann surface with the atlas given by the stereographic projection:

$$S^2 \setminus \{\infty\} \xrightarrow{z} \mathbf{C} \quad \text{and} \quad S^2 \setminus \{0\} \xrightarrow{\frac{1}{z}} \mathbf{C}.$$

3. Take a smooth affine plane curve $X = \{(x, y) \in \mathbf{C}^2 \mid f(x, y) = 0\}$, where $f \in \mathbf{C}[x, y]$ is such that for all $P \in X$ one of $\partial_x f(P), \partial_y f(P)$ does not vanish. Without loss of generality, suppose that $\partial_x f(P) \neq 0$. Then, by the holomorphic inverse function theorem the projection $P = (x, y) \mapsto y$ is a local homeomorphism from a neighborhood of P to an open subset of $\mathbf{C}$, and by the implicit function theorem these form an atlas.

3.1 Holomorphic functions

Definition 3.3. A *holomorphic map* between Riemann surfaces X and Y is a **non-constant** continuous map $\varphi \colon X \to Y$ such that on every chart $U \xrightarrow{f} \mathbf{C}$ of X and $V \xrightarrow{g} \mathbf{C}$ of Y such that $\varphi(U) \subset V$, the map

$$g \circ \varphi \circ f^{-1} \colon f(U) \to g(V)$$

is holomorphic.

Therefore, Riemann surfaces form a category where the morphisms are holomorphic maps $X \to Y$.

Example 3.4 (Holomorphic functions)**.** As a special case, if $Y = \mathbf{C}$ we say that a holomorphic map $X \to \mathbf{C}$ is a *holomorphic function* on X. The assignment

$$U \mapsto \{\text{holomorphic functions } U \to \mathbf{C}\}$$

where $U \subset X$ is open defines a sheaf, called the sheaf of holomorphic functions on X.

From now on, we will only consider non-constant holomorphic maps.

Proposition 3.5 (Local structure of holomorphic maps)**.** Let $\varphi \colon Y \to X$ be a holomorphic map of Riemann Surfaces, fix some $y \in Y$ and consider $x = \varphi(y) \in X$. Then, there exist open neighborhoods U_x of x and V_y of y such that $\varphi(V_y) \subset U_x$ and complex charts $f_x \colon U_x \to \mathbf{C}, g_y \colon V_y \to \mathbf{C}$ with $f_x(x) = 0$ and $g_y(y) = 0$ making the following diagram commute:

$$\begin{array}{ccc} V_y & \xrightarrow{g_y} & \mathbf{C} \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle z \mapsto z^{e_y}} \\ U_x & \xrightarrow{f_x} & \mathbf{C} \end{array}$$

for some integer $e_y \geq 1$ which does not depend on the charts chosen.

Proof. After performing some translations, we can assume that $f_x(x) = g_y(y) = 0$ and that $f_x \circ \varphi \circ g_y^{-1}$ is a holomorphic function in a neighborhood of 0. Therefore, by the Weierstrass preparation theorem we can write

$$f_x \circ \varphi \circ g_y^{-1} = z^{e_y} H(z)$$

for some holomorphic function H with $H(0) \neq 0$. By choosing a branch log of the complex logarithm in a neighborhood of $H(0)$, we can define

$$h := \exp\left(\frac{1}{e_y} \log \circ H\right),$$

which is holomorphic in $g_y(V_y)$ and satisfies $h^{e_y} = H$. Therefore, we get the result by composing g_y with $z \mapsto z \cdot h(z)$. □

This implies some purely topological properties of holomorphic maps between Riemann surfaces:

Corollary 3.6. In the above situation, φ is an open mapping with discrete fibres.

Proof. The map $z \mapsto z^{e_y}$ is open and being an open mapping is a local property, so φ is open. Moreover, the fibre $\varphi^{-1}(x)$ is discrete because in a neighborhood of each $y \in \varphi^{-1}(x)$, φ is finite-to-one. □

Definition 3.7. The points $y \in Y$ where $e_y \neq 1$ are called *branch points* of φ, and the value e_y is called the *ramification index* (or *branching order*) of φ at y.

Corollary 3.8. The set S_φ of branch points of φ in Y is a discrete closed subset.

Proof. By the above proposition, every $y \in Y$ has a punctured open neighborhood that contains no branch points. □

Definition 3.9. A continuous map $Y \xrightarrow{\varphi} X$ of topological spaces is *proper* if for every compact subset $K \subset X$, the inverse image $\varphi^{-1}(K)$ is compact in Y.

From now on, suppose that X and Y are locally compact Hausdorff topological spaces.

Lemma 3.10. Proper maps are closed.

Proof. Let $Z \subset Y$ be closed, and pick $x \in X \setminus \varphi(Z)$. We need to find an open neighborhood of x disjoint from $\varphi(Z)$. We know that there exists a compact neighborhood $\overline{V}$ of x such that $V = \operatorname{int}(\overline{V})$ is an open neighborhood of x. Since φ is proper, $\varphi^{-1}(\overline{V})$ is compact, and so $Z \cap \varphi^{-1}(\overline{V})$ is closed in a compact set, hence compact. Therefore, $\varphi(Z \cap \varphi^{-1}(\overline{V}))$ is compact and thus closed, so $V \setminus \varphi(\varphi^{-1}(\overline{V}) \cap Z)$ is open, disjoint from $\varphi(Z)$ and contains x. □

Example 3.11 (Examples)**.**

1. If X, Y are Hausdorff with Y compact, than any continuous map $Y \xrightarrow{\varphi} X$ is proper.
2. If X, Y are locally compact and $\varphi\colon Y \to X$ is a finite cover, then it is proper. Indeed, for any compact $Z \subset X$, choose an open covering $\mathcal{U}$ of $\varphi^{-1}(Z)$. By refining this covering, we can assume that φ is a trivial cover over every $U \in \mathcal{U}$. We can extract a finite covering of Z out of the $\varphi(U)$, whose preimages are a finite cover of $\varphi^{-1}(Z)$.

Proposition 3.12. Let $\varphi\colon Y \to X$ be a proper holomorphic map of Riemann surfaces with X connected and let S_φ be the set of branch points of φ. Then, φ is surjective with finite fibres, and its restriction to $Y \setminus \varphi^{-1}(\varphi(S_\varphi))$ is a finite topological cover of $X \setminus \varphi(S_\varphi)$.

Proof. Since φ is proper, its fibres are compact and discrete, hence finite. Morover, $\varphi(Y) \subset X$ is open by Corollary 3.6 and closed by the previous Lemma, so by connectedness of X we have $\varphi(Y) = X$. The fact that it is a cover follows from the local structure of holomorphic maps and the fact that

$$z \mapsto z^e\colon \mathbf{C} \setminus \{0\} \to \mathbf{C} \setminus \{0\}$$

is a finite cover. □

Notation. Let X be a connected Riemann surface and $S \subset X$ a discrete closed subset. We denote by $\mathrm{Hol}_{X,S}$ the category whose objects are proper holomorphic maps $Y \xrightarrow{\varphi} X$ of Riemann surfaces such that $\varphi(S_\varphi) \subset S$, and whose morphisms are holomorphic maps over X.

Theorem 3.13. The functor

$$(Y \to X) \longmapsto (Y \setminus \varphi^{-1}(S) \to X \setminus S)$$

induces an equivalence of categories

$$\mathrm{Hol}_{X,S} \longleftrightarrow \{ \text{ finite covers of } X \setminus S \ \}.$$

Lemma 3.14. Let X be a connected Riemann surface and $Y \xrightarrow{p} X$ a connected cover. Then, there exists a unique complex structure on Y such that p is holomorphic.

Proof. In particular, p is a local homeomorphism, so every $y \in Y$ has an open neighborhood V such that $p|_V$ is a homeomorphism onto its image $U = p(V)$. If $U' \to \mathbf{C}$ is a complex chart with $U' \subset U$ and $p(y) \in U'$, we can define a complex chart on y by

$$f \circ p : p^{-1}(U') \cap V \to \mathbf{C}.$$

□

Proof of Theorem 3.13. We start with essential surjectivity. Set $X' := X \setminus S$ and consider a finite cover $Y' \xrightarrow{\varphi'} X'$. By the previous lemma, Y' carries a complex structure. If we fix $x \in S$, we can find a complex chart mapping an open neighborhood U_x of x homeomorphically onto $D = \{|z| < 1\} \subset \mathbf{C}$. The restriction of φ' to $\varphi'^{-1}(U_x \setminus \{x\})$ is a finite cover with

$$(\varphi')^{-1}(U_x \setminus \{x\}) = \bigsqcup_{i \in I_x} V_x^i.$$

But then, by the structure of covers of the punctured disk on each V_x^i this cover is given by

$$D \setminus \{0\} \xrightarrow{z \mapsto z^k} D \setminus \{0\}$$

for some k. Now, for each $i \in I_x$ and each $x \in S$ fix an "abstract point" y_x^i, and set

$$Y := Y' \cup \{y_x^i : x \in S, i \in I_x\}.$$

We can then extend the map φ' to a map $Y \xrightarrow{\varphi} X$ by

$$\begin{aligned} \varphi \colon Y &\to X \\ y &\mapsto \begin{cases} \varphi'(y) & \text{if } y \in Y', \\ x & \text{if } y = y_x^i. \end{cases} \end{aligned}$$

Finally, define complex charts on Y via the atlas on Y' together with the charts obtained by extending the isomorphism $V_x^i \to U_x \setminus \{x\} \to D \setminus \{0\}$ to $V_x^i \cup y_x^i \to D$ by sending y_x^i to 0. One checks that this gives a complex structure on Y (and thus a topology) making φ holomorphic. Moreover, φ is proper because compact subsets in X differ from compacts in X' by finitely many points, and the same goes for Y. But then, since φ' is proper (being a finite cover) φ must be as well.

For full faithfulness, we must show that the association

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

from morphisms in $\mathrm{Hol}_{X,S}$ to morphisms of finite covers of X' is bijective. We already know that the map $Y' \to Z'$ is a cover, and that Y' carries a complex structure making it holomorphic and which is compatible with the one on Y by construction. We can then extend $Y' \to Z'$ to the points in $Y \setminus Y'$ by a similar argument as before. □

Definition 3.15. If $Y \xrightarrow{\varphi} X$ is a proper surjective map of locally compact Hausdorff spaces which restricts to a finite cover $Y' \to X' = X \setminus S$ with $S \subset X$ discrete closed, we call φ a *finite branched cover*. We say that φ is a *Galois branched cover* if $Y' \to X'$ is Galois.

Proposition 3.16. Let $\varphi\colon Y \to X$ be a proper holomorphic map of connected Riemann surfaces that is topologically a Galois branched cover. Then:

1. the automorphism group $\mathrm{Aut}(Y)$ acts transitively on **all fibres** of φ;

2. If $y \in Y$ is a branch point with ramification index e_y, then all points in the fibre $\varphi^{-1}(\varphi(y))$ are branch points with ramification index e_y, and the stabilizers of these points in $\mathrm{Aut}(Y|X)$ are cyclic of order e_y.

Proof. Point 1. follows by continuity of automorphisms, since we know that $\mathrm{Aut}(Y|X)$ acts transitively on all fibres that do not contain branch points.

For the second statement, note that an automorphism fixing some point y also stabilizes a small neighborhood around it, where by the local structure of holomorphic maps φ becomes $z \mapsto z^{e_y}$, for which we know the statement. □

3.2 Meromorphic functions and field theory

Definition 3.17. Let X be a Riemann surface. A *meromorphic function* on X is a holomorphic map $f\colon X \setminus S \to \mathbf{C}$ for some discrete closed subset $S \subset X$, such that on all charts $U \xrightarrow{\varphi} \mathbf{C}$ the composition $f \circ \varphi^{-1}$ gives a meromorphic function on $\varphi(U) \to \mathbf{C}$.

Meromorphic functions on X form a ring $\mathcal{M}(X)$.

Lemma 3.18. When X is connected, $\mathcal{M}(X)$ is a field.

Proof. Let $f \in \mathcal{M}(X)$ be nonzero. We have to prove that the zeros of f form a discrete subset, from which it follows that $\frac{1}{f}$ is meromorphic. Suppose not; then the zeros of f have some limit point x. Composing with a chart $U \xrightarrow{\varphi} \mathbf{C}$ such that $x \in U$, we get a meromorphic function $\varphi(U) \to \mathbf{C}$ whose zeros have a limit point, but then the identity theorem implies that f is identically 0. If we call A the set of those $x \in X$ such that f is identically 0 in a neighborhood of x, then A is open by definition and closed by the above argument, and since X is connected we conclude $A = X$, which contradicts the assumption that $f \neq 0$. □

Question: Are there non-constant meromorphic functions on a Riemann surface X?

Fact 3.19 (**Riemann existence theorem**)**.** If X is a compact connected Riemann surface and $x_1, x_2 \in X$ are distinct points, then there exists a meromorphic function on X which is holomorphic at x_1 and x_2 such that $f(x_1) \neq f(x_2)$.

Corollary 3.20. Let X be a compact connected Riemann surface, and consider $x_1, \ldots, x_n \in X$ distinct points. If $a_1, \ldots, a_n \in \mathbf{C}$ are arbitrary complex numbers, then there exists a meromorphic function f on X which is holomorphic at all x_i with $f(x_i) = a_i$ for all $i = 1, \ldots, n$.

Proof. It is enough to prove that that given $x_1, \dots, x_n$ there exists $f_j \in \mathcal{M}(X)$ such that $f_j(x_i) = \delta_{ij}$, for then we can take linear combinations. The case $n = 2$ follows from the Riemann existence theorem. The general case is then an easy induction. □

Let now $Y \xrightarrow{\varphi} X$ be a (proper) holomorphic map of Riemann surfaces. It induces a ring homomorphism

$$\begin{gathered}\mathcal{M}(X) \xrightarrow{\varphi^*} \mathcal{M}(Y) \\ f \mapsto f \circ \varphi.\end{gathered}$$

Suppose now that X, Y are compact Riemann surfaces with X connected.

Proposition 3.21. In this case, $\mathcal{M}(Y)$ is a finite étale $\mathcal{M}(X)$-algebra via φ^*.

Proof. If Y is non connected, then $Y = \bigsqcup_{i=1}^n Y_i$ with Y_i compact connected Riemann surfaces, and so $\mathcal{M}(Y) = \prod_{i=1}^n \mathcal{M}(Y_i)$ is a finite product of fields. Therefore, it's enough to prove that $\mathcal{M}(Y)$ is a finite field extension of $\mathcal{M}(X)$ when Y is connected. We actually prove something stronger, via the following proposition: □

Proposition 3.22. Let $\varphi \colon Y \to X$ be a holomorphic map of compact connected Riemann surface which has degree d as a branched cover. Then, $[\mathcal{M}(Y) : \mathcal{M}(X)] = d$.

We need the following lemma:

Lemma 3.23. In the above situation, any $f \in \mathcal{M}(X)$ satisfies a (not necessarily irreducible) polynomial equation $F(f) = 0$ with $F \in \mathcal{M}(X)[t]$ of degree d.

Proof of Proposition 3.22. We first show that there exists $f \in \mathcal{M}(Y)$ which satisfies an equation $F(f) = 0$ as in the Lemma with F *irreducible* of degree d. Let $x \in X$ be a point such that $\varphi^{-1}(x) = \{y_1, \dots, y_d\}$ does not contain branch points of φ. Then, by the Riemann existence theorem we can find $f \in \mathcal{M}(Y)$ such that $f(y_i) \neq f(y_j)$ for $i \neq j$ and f is holomorphic at all y_i. We can consider an irreducible factor $F \in \mathcal{M}(X)[t]$ of degree $\deg F \leq d$ of the polynomial coming from the Lemma such that $F(f) = 0$, and we claim that $\deg(F) = d$. Write $F = a_n t^n + \cdots + a_0$.

Case 1: All the $a_i \in \mathcal{M}(X)$ are holomorphic and not all zero at x. In this case, the complex polynomial $F_x \colon a_n(x)t^n + \cdots + a_0(x) \in \mathbf{C}(t)$ has d distinct roots, namely the $f(y_i)$'s, and this is only possible if $n = d$.

Case 2: In the general case, if one of the a_i is not holomorphic in x or 0 in x, we can move x a little bit in a small neighborhood so that all conditions are satisfied.

We now claim that $\mathcal{M}(Y) = \mathcal{M}(X)(f)$. Indeed, for the nontrivial inclusion take any $g \in \mathcal{M}(Y)$ and consider $\mathcal{M}(X)(f, g) \subset \mathcal{M}(Y)$. By the Theorem of the primitive element, there exists $h \in \mathcal{M}(Y)$ such that $\mathcal{M}(X)(f, g) = \mathcal{M}(X)(h)$. In particular, $M(X)(f) \subset \mathcal{M}(X)(h)$, but $[\mathcal{M}(X)(h) : \mathcal{M}(X)] \leq d$ by the Lemma, and so we have equality. □

Proof of Lemma (3.23). Take S_φ to be the set of branch points of φ, and suppose that $x \notin \varphi(S_\varphi)$. Then, x has an open neighborhood U such that $\varphi^{-1}(U) = \bigsqcup_{i=1}^d V_i$ with each V_i being mapped biholomorphically onto U. If $s_i : U \to V_i$ is the holomorphic section of $\varphi|_{V_i}$, for all i we set $f_i := f \circ s_i \in \mathcal{M}(U)$ and

$$F := \prod_{i=1}^{d} (t - f_i) = t^d + a_{d-1}t^{d-1} + \ldots + a_0,$$

where $a_i \in \mathcal{M}(U)$ and $F(f|_{\varphi^{-1}(U)}) = 0$ by construction. If $x_1 \notin \varphi(S_\varphi)$ is another point, we repeat the construction in a neighborhood U_1 of x_1 and get another polynomial $F_1 \in \mathcal{M}(U_1)[t]$ such that $F_1(f|_{\varphi^{-1}(U_1)}) = 0$. On the intersection $U \cap U_1$, both F and F_1 vanish at $f|_{\varphi^{-1}(U\cap U_1)}$, so they must be equal. Therefore, we can glue all these polynomials together to get an $F \in \mathcal{M}(X \setminus \varphi(S_\varphi))[t]$ such that $F(f|_{\varphi^{-1}(\varphi(S_\varphi))}) = 0$. We need to show that the a_i extend to functions in the whole $\mathcal{M}(X)$. Take $x \in \varphi(S_\varphi)$ and consider a chart $f_x \colon U_x \to \mathbf{C}$ with $x \in U_x$ and $f_x(x) = 0$. Then, $f_x \circ \varphi$ defines a holomorphic function in some neighborhood of each $y_i \in \varphi^{-1}(x)$ such that $f_x \circ \varphi(y_i) = 0$. Since $f \in \mathcal{M}(Y)$, there exists some $k > 0$ such that $(f_x \circ \varphi)^k \cdot f$ is holomorphic at all the y_i's. Composing with s_i, we get that every $f_x^k \cdot f_i$ is holomorphic and thus bounded on $U_x \setminus \{x\}$. The same holds for the $f_x^{kd} \cdot a_i$'s, since the coefficients a_i are symmetric polynomials in the f_i's. By Riemann's removable singularity theorem, the functions $f_x^{kd} \cdot a_i$ extend to holomorphic functions on U_x and are thus meromorphic functions on X, which implies that $F \in \mathcal{M}(X)[t]$. □

Fix now X to be a compact connected Riemann surface. We can define a contravariant functor by the rule $Y \mapsto \mathcal{M}(Y)$, by sending a morphism $Y \xrightarrow{\varphi} Z$ over X to the induced ring homomorphism $\mathcal{M}(Z) \xrightarrow{\varphi^*} \mathcal{M}(Y)$.

Theorem 3.24. This functor induces an anti-equivalence of categories

$$\left\{ \begin{array}{c} \text{holomorphic maps } Y \to X \\ \text{with } Y \text{ compact} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{finite étale} \\ \mathcal{M}(X)\text{-algebras} \end{array} \right\}$$

In this correspondence Galois branched covers correspond to Galois field extensions of $\mathcal{M}(X)$ of the same degree.

Example 3.25 (Case $X = \mathbb{P}^1_{\mathbf{C}}$)**.** If we consider the Riemann sphere $\mathbb{P}^1_{\mathbf{C}}$, then $\mathcal{M}(\mathbb{P}^1_{\mathbf{C}}) = \mathbf{C}(t)$ is the field of rational functions. By the Riemann Existence Theorem, there exists a non-constant $f \in \mathcal{M}(Y)$. Define $Y \xrightarrow{\varphi_f} \mathbb{P}^1_{\mathbf{C}}$ by

$$\varphi_f \colon Y \to \mathbb{P}^1_{\mathbf{C}}, \quad y \mapsto \begin{cases} f(y) & \text{if } f \text{ is holomorphic at } y, \\ \infty & \text{otherwise.} \end{cases}$$

It's easy to check that this is a holomorphic map (using the charts $z \mapsto z$ on $\mathbf{C}$ and $z \mapsto \frac{1}{z}$ on $\mathbb{P}^1_{\mathbf{C}} \setminus \{0\}$). This φ_f is a *proper* holomorphic map of compact Riemann surfaces, so by the above theorem $\mathcal{M}(Y)$ is a finite field extension of $\mathbf{C}(t)$. Therefore, "all compact Riemann surfaces are algebraic".

Corollary 3.26. The functor $Y \mapsto \mathcal{M}(Y)$ induces an anti-equivalence of categories between

$$\left\{ \begin{array}{c} \text{compact connected Riemann} \\ \text{surfaces} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{finitely generated field} \\ \text{extensions } K \text{ of } \mathbf{C} \text{ with } \operatorname{trdeg}_{\mathbf{C}} K = 1 \end{array} \right\}$$

Note that the right hand side consists of all finite field extensions of $\mathbf{C}(t)$.

Proof of Theorem 3.24. We start with essential surjectivity: it's enough to prove that for a finite extension $L|\mathcal{M}(X)$ there exists a connected compact $Y \to X$ such that $\mathcal{M}(Y) \cong L$. Write $L = \mathcal{M}(X)(\alpha)$ for some primitive element $\alpha \in L$, and let $F \in \mathcal{M}(X)[t]$ be its minimal polynomial over $\mathcal{M}(X)$ of degree d. Since F is separable, it and its derivative F' have no common roots in a PID, so $(F, F') = 1$ and thus there exist $A, B \in \mathcal{M}(X)[t]$ such that

$$AF + BF' = 1.$$

Notation. If $x \in X$ is a point where all the coefficients of F are holomorphic, we denote by $F_x[t]$ the complex polynomial obtained by evaluating the coefficients of F in x.

Notice that F_x and F'_x can have a common root if and only if the coefficients of A and B have a pole at x. So, if we define

$$S := \{\text{zeroes and poles of the coefficients of } F, A, B\} \subset X$$

and set $X' := X \setminus S$, then on X' the coefficients of F are holomorphic and for $x \in X'$ the polynomial F_x has d distinct roots.

Now, if $U \subset X'$ is an open subset, we associate to it the set

$$\mathcal{F}(U) := \{\text{holomorphic functions } f \text{ on } U \colon F(f) = 0\},$$

which defines a presheaf $\mathcal{F}$ of sets on X' with the restriction maps $f \mapsto f|_V$ for $V \subset U$ open. Notice that $\mathcal{F}$ is even a sheaf (since it consists of functions), and we claim that it is a locally constant sheaf. Indeed, if $x \in X'$, we know that $F_x \in \mathbf{C}[t]$ has d distinct roots $a_1, \dots, a_d$. In particular, $F'_x(a_i) \neq 0$ for all $i = 1, \dots, d$, so by the holomorphic version of the implicit function theorem there exists a holomorphic function f_i defined in a neighborhood of x such that $f_i(x) = a_i$ and $F(f_i) = 0$. Therefore, for a small enough connected neighborhood U of x we get $f_1, \dots, f_d \in \mathcal{F}(U)$ such that $F|_U \in \mathcal{M}(U)[t]$ factors as $\prod_{i=1}^d (t - f_i)$, because $\deg F = d$. This shows that $\mathcal{F}|_U$ is a constant sheaf of sets given by $\{f_1, \dots, f_d\}$.

To the sheaf $\mathcal{F}$ corresponds a cover $X'_{\mathcal{F}} \to X'$. It may not be connected, so let $Y'_1, \dots, Y'_r$ be its connected components. We know that for each Y'_j there exists a diagram

$$\begin{array}{ccc} Y'_j & \hookrightarrow & Y_j \\ \downarrow & & \vdots \\ X' & \hookrightarrow & X \end{array}$$

with the dotted arrow being a holomorphic map between compact Riemann surfaces extending the cover. If we set $Y := \bigsqcup_{j=1}^r Y_j$, we need show that $r = 1$ so that Y is connected. Define a function f on $X'_{\mathcal{F}}$ by sending $f_i \in \mathcal{F}_x$ to

$$f(f_i) := f_i(p(f_i)) \in \mathbf{C}. \tag{3.1}$$

By the same argument as in Lemma 3.23, f extends to a meromorphic function on each Y_j. The minimal polynomial G of f as a function on Y_j has degree d_j equal to the degree of the cover $Y'_j \to X'$. By construction we have $F(f) = 0$, which implies that G divides F but F is irreducible and so $d = d_j$ which means that $r = 1$ and Y is connected.

For full faithfulness, again it's enough to check it for connected covers. We fist show that for $Y \to X$ proper holomorphic, after restricting to X' we have an isomorphism between $Y' \to X'$ and the cover $X'_{\mathcal{F}} \to X'$ constructed above. It's easier to see that the associated locally constant sheaves are isomorphic, and if s_i is a local section, sending it to $f \circ s_i$ with f as in (3.1) gives the desired isomorphism. Thus, it suffices to show full faithfulness for the covers of the form $X'_{\mathcal{F}} \supset Y$ as above. By essential surjectivity, it's enough to consider a diagram of field extensions of the form

$$\begin{array}{ccc} \mathcal{M}(X'_{\mathcal{F}}) & \longleftarrow & \mathcal{M}(X'_{\mathcal{G}}) \\ & \nwarrow \quad \nearrow & \\ & \mathcal{M}(X') & \end{array} .$$

This means that $\mathcal{M}(X'_{\mathcal{F}}) \subset \mathcal{M}(X'_{\mathcal{G}}) \subset \mathcal{M}(Y')$. By construction, there exists a unique morphism of covers which fits in the diagram

$$\begin{array}{ccc} X'_{\mathcal{F}} & \dashrightarrow & X'_{\mathcal{G}} \\ & \searrow \quad \swarrow & \\ & X' & \end{array}$$

inducing the above diagram of field extensions.

Finally we have to show that Galois branched covers correspond to Galois field extensions. Notice that by full faithfulness

$$\mathrm{Aut}(Y|X) \cong \mathrm{Aut}(\mathcal{M}(Y)|\mathcal{M}(X)),$$

and recall that $\deg Y = [L : \mathcal{M}(X)]$. Therefore, both groups have order $\leq d$, and equality holds if and only if the cover (resp. field extension) is Galois and the result follows by counting orders. □

3.3 The absolute Galois group of $\mathbf{C}(t)$

Let X be a compact connected Riemann surface. For $S \subset X$ finite, set $X' := X \setminus S$ and fix an algebraic closure $\overline{\mathcal{M}(X)}$ of $\mathcal{M}(X)$. We define $K_{X'}$ to be the composite, inside $\overline{\mathcal{M}(X)}$, of all finite subextensions which correspond (by the previous theorem) to $Y|X$ where Y restricts to a cover over X'.

Note. The extension $K_{X'}|\mathcal{M}(X)$ is Galois, because if $K_{X'} \supset L \supset \mathcal{M}(X)$ is a finite subextension and $\sigma \in \mathrm{Gal}(\overline{\mathcal{M}(X)}|\mathcal{M}(X))$, then $\sigma(L) \subset K_{X'}$ by construction.

Theorem 3.27. The extension $K_{X'}|\mathcal{M}(X)$ is Galois, with Galois group

$$\mathrm{Gal}(K_{X'}|\mathcal{M}(X)) \cong \pi_1\widehat{(X', x)}$$

for some $x \in X'$.

Example 3.28 (Case $X = \mathbf{P}^1_{\mathbf{C}}$)**.** Take $S = \{x_1, \dots x_n\}$ and set

$$X' = \mathbf{P}^1_{\mathbf{C}} \setminus S \cong \mathbf{C} \setminus \{x_1, \dots x_{n-1}\}.$$

Then, we have

$$\pi_1(X', x) \cong \text{free group on } (n-1) \text{ generators},$$

and we can also express the fundamental group via the presentation

$$\langle \gamma_1, \dots, \gamma_n | \gamma_1 \cdot \dots \cdot \gamma_n = 1 \rangle$$

where γ_i is the class of a loop going around x_i.

Therefore, every finite group which can be generated by $n-1$ elements arises as a quotient of $\pi_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{x_1, \dots, x_n\}, x)$.

Corollary 3.29. If G is a finite group, then there exists a finite Galois extension $L|\mathbf{C}(t) = \mathcal{M}(\mathbf{P}^1_{\mathbf{C}})$ such that $\mathrm{Gal}(L|\mathbf{C}(t)) \cong G$.

Proof. If G can be generated by $n-1$ elements, then G is a quotient of $\pi_1(X', x)$ with $X' = \mathbf{P}^1_{\mathbf{C}} \setminus \{x_1, \dots, x_n\}$, and by the Theorem we have

$$\pi_1(X', x) \cong \mathrm{Gal}(K_{X'}|\mathcal{M}(\mathbf{P}^1_{\mathbf{C}})) \twoheadleftarrow \mathrm{Gal}(\overline{\mathbf{C}(t)}|\mathbf{C}(t)).$$

□

Remark 3.30. The above Corollary actually proves that if a finite group G can be generated by $n-1$ elements, then $G \cong \mathrm{Aut}(Y|\mathbf{P}^1_{\mathbf{C}})$ where Y is a branched cover ramified only over n points $x_1, \dots, x_n \in \mathbf{P}^1_{\mathbf{C}}$.

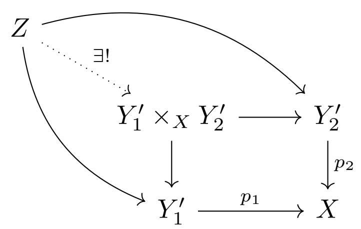
Complement. Under the surjection $\pi_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{x_1, \dots, x_n\}) \twoheadrightarrow G$, the image of each generator γ_i generates the stabilizer of a branch point in $p^{-1}(x_i)$. The main point is that in some neighborhood U_i of x_i the map $Y \to X$ becomes isomorphic to the branched cover of the unit disk given by $z \mapsto z^{e_i}$. So, locally over U_i it looks like $V_i \setminus \{y_i\} \to U_i \setminus \{x_i\}$ and

$$\mathrm{Aut}(V_i|U_i) \cong \mathbf{Z}/e_i\mathbf{Z} \cong \langle \gamma_i \rangle / e_i \langle \gamma_i \rangle.$$

Proof of Theorem 3.27. We first want to understand the composite of two finite subextensions $L_1, L_2 \subset \overline{\mathcal{M}(X')}$ as in the theorem. These correspond to covers $Y'_1 \xrightarrow{p_1} X$ and $Y'_2 \xrightarrow{p_2} X$. Recall that the fibre product $Y'_1 \times_X Y'_2$ is defined as

$$Y'_1 \times_X Y'_2 := \{(y_1, y_2) \in Y'_1 \times Y'_2 \colon p_1(y_1) = p_2(y_2)\},$$

and notice that it can also be characterized by the universal property that for any Z with maps to Y'_1 and Y'_2 over X, there exists a unique map making the following diagram commute:



Now, the corresponding universal property for the analogous diagram obtained applying $M(-)$ to the above diagram is satisfied by the tensor product $L_1 \otimes_{\mathcal{M}(X)} L_2$. If $L_2 = \mathcal{M}(X)[\alpha]$ and f is the minimal polynomial of α over $\mathcal{M}(X)$, then we have $L_1L_2 = L_1(\alpha)$ and

$$L_2 \cong \mathcal{M}(X)[t]/(f) \implies L_1 \otimes_{\mathcal{M}(X)} L_2 \cong L_1[t]/(f).$$

Therefore, if f factors as $f = f_1 \cdots f_r$ over L_1, we have

$$L_1 \otimes_{\mathcal{M}(X)} L_2 \cong \bigoplus_{j=1}^{r} L_1[t]/(f_j),$$

and L_1L_2 will correspond to the factor where $f_j(\alpha) = 0$. In conclusion, to obtain the surface corresponding to the composite L_1L_2, we have to extend the connected component of $Y_1' \times_X Y_2'$ corresponding to the factor described above to a compact Riemann surface.

Lemma 3.31. If $K_{X'} \supset K \supset \mathcal{M}(X)$ is a finite subextension, then $K = \mathcal{M}(Z)$ where $Z \to X$ is a compact Riemann surface that restricts to a cover over X'.

Proof. We first find $L_1, \dots, L_r$ as in the definition of $K_{X'}$ such that $K \subset L_1 \cdots L_r$. By the previous argument, we get that $L_1 \cdots L_r = \mathcal{M}(\widetilde{Z})$ with $\widetilde{Z}$ restricting to a cover over X'. So, we have to show that if $\mathcal{M}(\widetilde{Z}) \supset K \supset \mathcal{M}(X)$ are finite extensions, then $K = \mathcal{M}(Z)$ for some $Z \to X$ restricting to a cover over X'. If $d = [K : \mathcal{M}(X)]$ and $e = [\mathcal{M}\widetilde{Z}) : K]$, we know that $K = \mathcal{M}(Z)$ for some compact Riemann surface $Z \to X$. If we fix $x \in X'$, x has $d \cdot e$ preimages in $\widetilde{Z}$ and $z_1, \dots, z_r$ preimages in Z with $r \leq d$. Moreover, each z_i has $\leq e$ preimages in $\widetilde{Z}$. By counting, we must have equality everywhere, and we are done. □

Finally, let G be a finite quotient of $\pi_1(X', x)$. We know that G corresponds to a finite Galois cover $Y' \to X'$, which extend to a holomorphic map $Y \to X$ of compact Riemann surfaces that is Galois as a branched cover, which restricts to $Y' \to X'$. This in turn corresponds to a finite quotient of $\mathrm{Gal}(K_{X'}|\mathcal{M}(X))$. In this way, we get a bijection between the finite quotients of $\pi_1(X', x)$ and finite quotients of $\mathrm{Gal}(K_{X'}|\mathcal{M}(X))$ which is compatible with the respective inverse systems, and so it implies the desired isomorphism of profinite groups. □

Definition 3.32. Let X be a set. The free profinite group $\widehat{F}(X)$ with basis X is defined by the following universal property: for any map $X \xrightarrow{\lambda} G$ with G profinite such that all open normal subgroups $U \lhd G$ contain all but finitely many elements of $\lambda(X)$, there exists a unique factorization

$$\begin{array}{ccc} X & \longrightarrow & \widehat{F}(X) \\ & \searrow^{\lambda} & \downarrow {\scriptstyle \exists ! \tilde{\lambda}} \\ & & G \end{array}$$

where $\tilde{\lambda}$ is a map of profinite groups.

To see that such a group exists, take the free group $F(X)$ with basis X and define

$$\widehat{F}(X) := \varprojlim_{\substack{U \lhd F(X) \\ [F(X):U]<\infty \\ U \text{ contains all but finitely many } x\in X}} F(X)/U.$$

Theorem 3.33 (Douady)**.** The group $\mathrm{Gal}(\overline{\mathbf{C}(t)}|\mathbf{C}(t))$ is isomorphic to the free profinite group with basis $\mathbf{C}$.

Idea of the Proof. Let $S \subset \mathbf{C}$ be a finite subset of cardinality r, and set

$$X_S := \mathbf{P}^1_{\mathbf{C}} \setminus (S \cup \{\infty\}) = \mathbf{C} \setminus S.$$

Then, we have seen that

$$\mathrm{Gal}(K_{X_S}|\mathbf{C}(t)) \cong \widehat{F_r},$$

whose topological generators are given by loops γ_i around the points of S.

If $S \subset T \subset \mathbf{C}$ are both finite, then $K_{X_S} \subset K_{X_T}$ induces a map

$$\lambda_{ST}\colon\ \mathrm{Gal}(K_{X_T}|\mathbf{C}(t)) \twoheadrightarrow \mathrm{Gal}(K_{X_S}|\mathbf{C}(t))$$

which sends all loops around a point not in S to the identity. By Theorem 3.24, we know that K_{X_S} are cofinal among all finite subextensions of $\overline{\mathbf{C}(t)}|\mathbf{C}(t)$, so we have

$$\mathrm{Gal}(\overline{\mathbf{C}(t)}|\mathbf{C}(t)) \cong \varprojlim_S \mathrm{Gal}(K_{X_S}|\mathbf{C}(t)).$$

The proof is then reduced to the following group-theoretic proposition: □

Proposition 3.34. Let X be a set and consider

$$\mathcal{S} = \{\text{finite subsets } S \subset X\}$$

partially ordered by inclusion. If (G_S, λ_{ST}) is an inverse system of profinite groups indexed by $\mathcal{S}$ such that

1. $\lambda_{ST}\colon G_T \to G_S$ is surjective
2. every G_S has a system $\{g_x \colon x \in S\}$ of elements such that the induced map

   $$\begin{aligned} \widehat{F}(S) &\to G_S \\ (x \in S) &\mapsto g_x \end{aligned}$$

   is an isomorphism and $\lambda_{ST}(g_x) = 1$ if $x \notin S$.

Then,

$$\varprojlim_S G_S \cong \widehat{F}(X).$$

For this, we need a few lemmas.

Lemma 3.35. The proposition holds in the case when $G_S = \widehat{F}(S)$ for all S and λ_{ST} is given by

$$\lambda_{ST}(x) = \begin{cases} x, & x \in S \\ 1, & x \notin S \end{cases}$$

Proof. We check the universal property defining $\widehat{F}(X)$. First observe that there is a natural injection $\hat{\imath}: X \to \varprojlim \widehat{F}(S)$ sending $x \in X$ to $(x_S)_{S\in\mathcal{S}}$, where $x_S = x$ for $x \in S$ and $x_S = 1$ otherwise. It generates a dense subgroup in $\varprojlim \widehat{F}(S)$, so given a map $\lambda: X \to G$ with G finite, an extension $\varprojlim \widehat{F}(S) \to G$ must be unique if exists. But since G is finite, we must have $\lambda(x) = 1$ for all but finitely many $x \in X$, so λ factors through the image of $\hat{\imath}(X)$ in some quotient $\widehat{F}(S)$, which is none but S. The existence then follows from the freeness of $\widehat{F}(S)$. □

Lemma 3.36. If $|X| = r < \infty$, then in $\widehat{F}(X)$ every system of r topological generators is a basis.

Proof. By assumption the map $i_F : \widehat{F}(S) \to \widehat{F}(X)$ is surjective, so it is enough to show injectivity. For each $n > 0$ consider the sets $Q_n(S)$ (resp. $Q_n(X)$) of open normal subgroups of index n in $\widehat{F}(S)$ (resp. $\widehat{F}(X)$). As $\widehat{F}(S)$ and $\widehat{F}(X)$ are both profinite free of rank r, these sets have the same finite cardinality (bounded by $(n!)^r$). By surjectivity of i_F the map $Q_n(X) \to Q_n(S)$ sending $U \subset \widehat{F}(X)$ to $i_F^{-1}(U)$ is injective, hence bijective. It follows that $\ker(i_F)$ is contained in all subgroups in $Q_n(S)$, for all $n > 0$. As $\widehat{F}(S)$ is profinite, this means $\ker(i_F) = \{1\}$.

□

Lemma 3.37. The inverse limit of an inverse system of nonempty compact topological spaces is nonempty.

Proof. Let $X_\alpha, \varphi_{\alpha\beta}$ be such an inverse system. Consider the closed subset $X_{\lambda\mu} \subset \prod_\alpha X_\alpha$ consisting of sequences (x_α) with $\varphi_{\lambda\mu}(x_\mu) = x_\lambda$ for $\lambda \le \mu$ fixed, then

$$\varprojlim_\alpha X_\alpha = \bigcap X_{\lambda\mu}$$

As the intersection of finitely many $X_{\lambda\mu}$'s is nonempty (because X_α is indexed by a directed set), we conclude by compactness. □

Proof of Proposition 3.34. Let $S \in \mathcal{S}$ and set $r := |S|$. If we set

$$B_S := \{(g_1, \dots, g_r) \in G_S^r\}$$

where the topological generators g_i are as in property (2) of the proposition. One sees that $B_S \subset G_S^r$ is closed and nonempty. Since G_s^r is a product of compact spaces, B_S is also compact, and thus by Lemma 3.37 we get

$$\varprojlim_S B_S \neq \emptyset.$$

By construction and Lemma 3.36, an element in the above inverse limit induces an isomorphism of the inverse system of Lemma 3.35 with (G_S, λ_{ST}), and we conclude by that lemma. □

References

[1] Serge Lang, *Algebra*, 3rd edition, Addison-Wesley, 1993.

[2] L. Ribes and P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, Springer Berlin Heidelberg, 2010.

[3] R. Kucharczyk, P. Scholze, Topological realisations of absolute Galois groups, in *Cohomology of arithmetic groups*. Springer, 2018, 201–288.