Lectures On Galois Groups and Fundamental Groups

Tamás Szamuely, notes by Francesco Minnocci

Contents

1 Galois theory of fields **2**
1.1 Basic notions 2
1.2 Profinite groups and their topology 4
1.3 The Galois correspondence 6
1.4 Grothendieck's Galois theory 9

2 Topological Covers **14**
2.1 Galois theory of Covers 14
2.2 Monodromy and the Universal Cover 17

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

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

   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 Haussdorff), 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

$$\begin{tikzcd} \mathrm{Gal}(K|k) \arrow[r] \arrow[dr, dotted] & \prod_L \mathrm{Gal}(L|k) \arrow[d, "\pi_L"] \\ & \mathrm{Gal}(L|k) \end{tikzcd}$$

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
$$\begin{aligned} L &\longmapsto H = \mathrm{Gal}(K|L) \\ H &\longmapsto K^H \end{aligned}$$
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 $\varphi : \overline{K}_1 \xrightarrow{\sim} \overline{K}_2$ 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 $U_L := \varphi_M^{-1}(\mathrm{Gal}(M|L)) \subset \mathrm{Gal}(K|k)$ 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 $L := K^H$. 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 fiber

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

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 fiber

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

is open. We can write

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

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

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

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:
$$\begin{tikzcd} V \arrow[r, "\varphi"] & W \\ F(A) \arrow[u, "i_V", "\cong"'] \arrow[r, "i_W \circ f \circ i_V^{-1}"] & F(B) \arrow[u, "i_W"', "\cong"] \end{tikzcd}$$
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:

$$\begin{tikzcd} k_s^V \arrow[r, hook] & k_s^U \\ f(\varphi)(L) \arrow[u, "\cong"] \arrow[r, dashed] & \varphi(M) \arrow[u, "\cong"'] \\ L \arrow[u, "\cong"] \arrow[r, dashed] & M \arrow[u, "\cong"'] \end{tikzcd}$$

$\square$

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 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 fiber 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 $Y \to X$ is a morphism between connected covers of X, then f is itself a Galois cover and $Z \cong Y/H$ with $H = \mathrm{Aut}(Y|Z)$.

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. $\square$

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

$$\begin{tikzcd} Y \arrow[rr, "p_Y"] \arrow[dr, "p"'] & & Z \arrow[dl, "p_2"] \\ & X & \end{tikzcd}$$

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 $Y \to X$ and $Z \to X$ are covers, then $Y \to Z$ is a cover.

Sketch of proof. For every z in Z, set $x := p_2(z)$ 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 $p_Y(U_i) = V_j$, and a little reflection shows that p_Y is surjective.

$\square$

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 $p_Y \circ \varphi$. $\square$

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

$$\left\{ \text{ subgroups } H \leq \mathrm{Aut}(Y|X) \right\} \longleftrightarrow \left\{ \text{ connected covers } \begin{tikzcd} Y \arrow[rr] \arrow[dr] & & Z \arrow[dl] \\ & X & \end{tikzcd} \right\}.$$

Proposition 2.18. In the above correspondence, normal subgroups $H \triangleleft \mathrm{Aut}(Y|X)$ correspond to Galois covers $Z \to X$, and in this case

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

Proof. If H is normal in $G := \mathrm{Aut}(Y|X)$, 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

$$\begin{tikzcd}
Y \arrow[r, "\phi"] \arrow[d, "p_Y"] & Y \arrow[d, "p_Y"] \\
Z \arrow[r, dashed, "\psi"] \arrow[d, "p_2"] & Z \arrow[d, "p_2"] \\
X \arrow[r, equal] & X
\end{tikzcd}$$

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 $f \cdot g$ 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 basepoint x in X. We define a functor

$$\mathrm{Fib}_x \colon \{\text{covers of } X\} \to \{\text{sets with a left } \pi_1(X, x)\text{-action}\}$$

which sends $p \colon Y \to X$ to the fiber $p^{-1}(x)$ of the base point, with the monodromy action. To a morphism $f \colon Y_1 \to Y_2$ of covers we associate $f|_{p_{Y_1}^{-1}(x)} \colon p_{Y_1}^{-1}(x) \to p_{Y_2}^{-1}(x)$, 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

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

Here 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

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

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 also straightforward. □

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

Definition 2.25. 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

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

Proposition 2.26. $\widetilde{X}_x$ 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 2.27. 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 2.28. 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, $f \coloneqq p \circ \tilde{f}$ 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 2.29. 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 2.26. We want to show that $\widetilde{X}_x \to X$ is a Galois cover. By Lemma 2.27, 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 that π_y is a connected cover, in particular it is surjective. Take some $\tilde{z} \in \pi_{\tilde{y}}(\tilde{x})$. Again, by representability we get a morphism of covers $\pi_{\tilde{z}} \colon \widetilde{X}_x \to \widetilde{X}_x$ such that $\pi_{\tilde{z}}(\tilde{x}) = \tilde{z}$. Furthermore, $\pi \circ \pi_{\tilde{y}} \circ \pi_{\tilde{z}} = \pi$, so by Lemma 2.8 we have

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

but since these are surjective maps, this shows injectivity of $\pi_{\tilde{y}}$ and we conclude that $\pi_{\tilde{y}}$ is an automorphism of covers.

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

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

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 $f^{-1} \cdot g$ in $\pi_1(X,x)$. The associated ϕ_α coincides with ϕ in $\tilde{x}'$, so they are equal by the usual lemma. $\square$

Propositions 2.23 and 2.26 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

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

References

[1] S. Lang. *Algebra.* Addison-Wesley, 3 edition, 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.