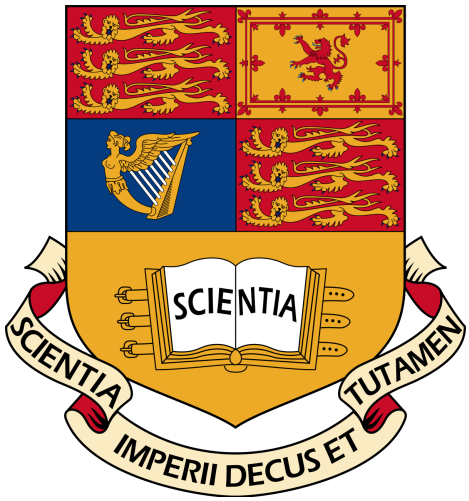
CID: 01112508 Supervisor: Prof. A. N. Skorobogatov

Galois Categories

Sjoerd de Vries

M3R

Spring 2018



This is my own work unless otherwise stated.

Abstract

First conceived by Grothendieck in his SGA, the theory of Galois categories is a beautiful generalisation of classical Galois theory which allows one to generalise Galois theory to settings other than fields. Most notably, one can use this to define the étale fundamental group of a scheme. Moreover, the theory makes precise the relationship between the Galois group of a field and the fundamental group of a (suitable) topological space: they both arise as the automorphism group of a fundamental functor.

Contents

Contents

0 Introduction

The aim of this report is to give a self-contained introduction to Galois categories. For some reason, this theory is not (yet) easily accessible: it was originally introduced in Grothendieck's SGA [6], and an adaptation can be found in Lenstra's Galois Theory for Schemes [9]. However, due to the nature of these sources, they call for much more background knowledge than is strictly necessary, and will not be suitable for readers who just want to learn about Galois categories. As a result, while [6] and [9] were the main sources for this report and many results may be found in either one of these, there is a sharp distinction in presentation.

After a brief run-through of some preliminaries in Section 1, we start off with a discussion of basic category theory in Section 2, focusing on the notions needed to introduce Galois categories. Section 3 gives an overview of the properties of Galois categories, and it is in this section that we prove the main results. In particular, we will prove the following theorem:

Theorem 0.1 (Grothendieck)**.** Let $(\mathcal{C}, F)$ be a Galois category. Then $\mathcal{C}$ is equivalent to the category π-FSet of finite sets equipped with a continuous π-action, where π is a profinite group and the finite sets are given the discrete topology.

In Section 4, we give two important examples of Galois categories, with the aim to justify the previously developed theory.

Category theory can be very abstract – at times, it seems too much so: if notions are too general, we cannot reasonably assume to deduce anything interesting from them. For this reason, this report contains many examples, which should help motivate and clarify the definitions. Such examples may be quite long, and for clarity the end of an example is indicated by a lozenge (⧫). This abstraction does have its merits: category theory gives a bird's-eye view of mathematics, and allows us to see connections between seemingly unrelated concepts. For instance, we will see that Galois groups and fundamental groups both arise as the automorphism group of the fundamental functor of a Galois category.

Of course, none of the theory in this report is my own. However, there is some originality: aside from the presentation mentioned before, this report contains several results which I have not been able to find anywhere, except perhaps in the form of an exercise in a book. Some of the examples are original as well, although the category theory in this report is sufficiently well-studied that I would be very surprised if these were not already documented elsewhere.

I would like to thank Professor Skorobogatov for his supervision of this project, and everyone else I have had meaningful discussions with: for me, discussing mathematics is what makes it all worthwhile.

1 Preliminaries

We start with a brief overview of some notions from group theory which play an important role in this report, namely group actions and profinite groups.

1.1 Group actions

Definitions 1.1.
1. If G is a group with a topology such that the group operation and inversion are continuous with respect to this topology, we say G is a *topological group*.
2. Let G be a group and X a set. A *group action* is a function $G \times X \to X$ such that $ex = x \ \forall x \in X$ and $(gh)x = g(hx)$ for all $g, h \in G$ and $x \in X$.
3. We say the action is *transitive* if X is non-empty and for each $(x, y) \in X^2$ there exists $g \in G$ such that $gx = y$.
4. We say the action is *free* if for any $x \in X$, $gx = hx \implies g = h$.
5. If X is a topological space and G is a topological group, we say that the group action is *continuous* if the group action is a continuous map $G \times X \to X$.
6. Let G be a group acting on a set X. For any $x \in X$, define the *stabilizer* of x to be $\mathrm{Stab}(x) = \{g \in G \mid gx = x\} \leq G$.
7. Let G be a group acting on a set X. For any $x \in X$, define the *orbit* of x as $Gx = \{gx \mid g \in G\}$.

We can take the quotient of a set by a group action: there is an equivalence relation $\sim$ on X given by $x \sim y \iff gx = y$ for some $g \in G$, and we define $X/G := X/\!\sim$. Of course, this is nothing else than the set of orbits.

Proposition 1.2. Let G and X be finite. If G acts freely on X, then $|X/G| = |X|/|G|$. If the action is transitive as well, then $|X| = |G|$.

Proof. For any $x \in X$, $|Gx| = |G|$ since the action is free. Thus, $\sim$ partitions X into equivalence classes of size $|G|$, yielding $|X|/|G|$ equivalence classes, i.e. $|X|/|G|$ orbits. If the action is transitive, there is exactly one orbit, and $|X| = |G|$. □

The following well-known theorem makes precise the relationship between orbits and stabilizers.

Theorem 1.3 (Orbit-Stabilizer)**.** Let G be a finite group acting on a set X. Then for any $x \in X$,

$$|Gx| = [G : \mathrm{Stab}(x)] = |G|/|\mathrm{Stab}(x)|.$$

Proof. Let $x \in X$, and let $\phi : G \to Gx$ be the set-function mapping $g \mapsto gx$. By definition of Gx, ϕ is surjective, and if $g^{-1}h \in \mathrm{Stab}(x)$, then $\phi(g) = gx = gg^{-1}hx = hx = \phi(h)$. Conversely, $\phi(g) = \phi(h) \implies g^{-1}h \in \mathrm{Stab}(x)$, and it follows that the quotient map $\tilde{\phi} : G/\mathrm{Stab}(x) \to Gx$ is a bijection of finite sets. The theorem follows. □

Proposition 1.4. Let G be a topological group acting on a discrete topological space X. The action of G is continuous if and only if $\mathrm{Stab}(x)$ is open in G for all $x \in X$.

Proof. First, suppose G acts continuously on X. For any $x \in X$, we have a continuous map $i_x : G \to G \times X$ sending $g \mapsto (g, x)$. Composing this map with the group action, we obtain continous maps $\phi_x : G \to X$ sending $g \mapsto gx$. $\mathrm{Stab}(x)$ is the pre-image of x under ϕ_x and since X is discrete, $\mathrm{Stab}(x)$ is open in G.

Conversely, suppose $\mathrm{Stab}(x)$ is open in G for all x. By discreteness of X, it suffices to show that $U_x = \{(g, y) \in G \times X \mid gy = x\}$ is open for all x. We have

$$U_x = \bigcup_{y \in X} \{(g, y) \mid g \in G,\ gy = x\},$$

but each of these sets is either empty or homeomorphic to $\mathrm{Stab}(y)$ via the map $h \mapsto (gh, y)$ for some g such that $gy = x$. Thus, U_x is open as a union of open sets and the action is continuous. □

1.2 Profinite groups

Profinite groups are a special kind of topological groups. Suppose we have a collection of finite groups $(G_i)_{i \in I}$ for some index set I. If I comes with some ordering $\geq$ which is directed in the sense that for any $i, j \in I$, there exists $k \in I$ with $k \geq i$ and $k \geq j$, and if for each $i \geq j$ there is a homomorphism $\phi_{ij} : G_i \to G_j$ such that $\phi_{ik} = \phi_{jk} \circ \phi_{ij}$ for each $i \geq j \geq k$, we say that the 2-tuple $((G_i)_{i \in I}, \{\phi_{ij}\})$ is an *inverse system*. Each inverse system has a group associated to it, which we call the *inverse limit*, denoted $\varprojlim G_i$. The inverse limit is a topological group which is constructed as follows.
Endow each of the finite groups G_i with the discrete topology, and $G = \prod_{i \in I} G_i$ with the product topology. The inverse limit is defined to be the subset of G consisting of those elements which are compatible with the maps ϕ_{ij}; that is,

$$\varprojlim G_i = \{(g_i)_{i \in I} \in \prod_{i \in I} G_i \mid \phi_{ij}(g_i) = g_j \text{ whenever } i \geq j\}.$$

When we endow the inverse limit with the subspace topology, it turns into a topological subgroup of the product space G. The fact that it is a subgroup follows because the ϕ_{ij} are group homomorphisms. When referring to the "compatibility requirement" or "compatibility property" of inverse systems, we mean the property that $\phi_{ik} = \phi_{jk} \circ \phi_{ij}$.
The topology on the inverse limit is called the *profinite topology*. Groups endowed with the profinite topology are called *profinite groups*. Profinite groups have an equivalent definition:

Theorem 1.5. Let G be a topological group. Then G is profinite if and only if G is Hausdorff, compact, and totally disconnected.

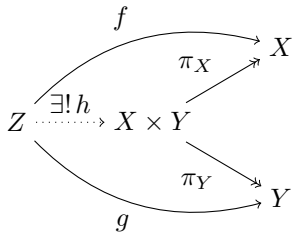
For a full proof, see [14]. As a corollary, we obtain that any closed subgroup of a profinite group is itself profinite.

2 Basic Category Theory

2.1 Categories

In order to make precise the relationship between Galois groups and fundamental groups, we will need the language of category theory. The main idea behind categories is that we should not think about objects (e.g. sets, groups, topological spaces) in themselves, but rather about the maps between such objects. Once we have set up this language, we will be able to formulate what exactly we mean when we say two things are "the same". We will often make use of *commutative diagrams*. These are schematic renditions of maps between objects which are compatible with each other: following different arrows to the same object gives the same result.

A motivating example: let X and Y be sets, $X \times Y$ their Cartesian product, and π_X, π_Y the projections onto the respective coordinates: that is, $\pi_X(x, y) = x$, $\pi_Y(x, y) = y$. If Z is any other set, giving set-functions $f : Z \to X$, $g : Z \to Y$ is the same as giving a set-function $h : Z \to X \times Y$, in the sense that one can uniquely construct h from f and g, and obtain f and g from h: indeed, we have $f = \pi_X \circ h$ and $g = \pi_Y \circ h$, forcing $h(z) = (f(z), g(z))$. We can summarise this in the following commutative diagram:



Here two-headed arrows indicate surjectivity; injectivity is indicated by hooked arrows ($\hookrightarrow$).
The Cartesian product (equipped with the projection maps) actually satisfies a *universal property* in the category of sets, namely the universal property of products. Other examples of products are direct products in the category of groups, and the Segre embedding in the category of algebraic varieties. But let us not get ahead of ourselves. In order to properly talk about these notions, we first have to know what a category is.

Definition 2.1. A *category* $\mathcal{C}$ is a collection of *objects* of $\mathcal{C}$, denoted $\mathrm{Obj}(\mathcal{C})$, and, for any two objects A and B in $\mathrm{Obj}(\mathcal{C})$, a collection of *morphisms* between them, denoted $\mathrm{Hom}_{\mathcal{C}}(A, B)$, obeying the following axioms:

1. For any object A of $\mathcal{C}$, there is a morphism $\mathrm{Id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$;
2. For any objects A, B, C of $\mathcal{C}$, whenever $\phi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and $\psi \in \mathrm{Hom}_{\mathcal{C}}(B, C)$, there exists a morphism $\psi \circ \phi \in \mathrm{Hom}_{\mathcal{C}}(A, C)$ such that the following hold:
   - $\forall \phi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ we have $\phi \circ \mathrm{Id}_A = \phi = \mathrm{Id}_B \circ \phi$;
   - This "composition" is associative, i.e. $\phi \circ (\psi \circ \chi) = (\phi \circ \psi) \circ \chi$ whenever such compositions make sense;
3. $\mathrm{Hom}_{\mathcal{C}}(A, B) \cap \mathrm{Hom}_{\mathcal{C}}(C, D) = \emptyset$ unless $A = C$ and $B = D$.

If we have $\phi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ such that there exists $\psi \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ such that $\psi \circ \phi = \mathrm{Id}_A$ and $\phi \circ \psi = \mathrm{Id}_B$, we say ϕ is an *isomorphism*.

The third property is almost always trivial, and we will usually ignore it. For our purposes, morphisms can always be thought of as functions of some sort, but of course nothing stops us from considering other kinds of objects as morphisms.
There are many examples of categories. The following list is by no means exhaustive, but is intended to give a good idea of the kind of categories we will be working with.

Examples 2.2.
1. The category we were working in earlier was the category of sets, which we can now verify to indeed be a category. This category, which we will call Set, may be the most intuitive example of category there is, as the morphisms are just the familiar set-functions. One thing worth emphasising, though, is that $\mathrm{Obj}(\mathsf{Set})$ is the collection of all sets, which itself is not a set, as Russell's paradox tells us. In general, objects of a category form a *class*. We say a category is *small* if $\mathrm{Obj}(\mathcal{C})$ is a set and $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is a set for all $A, B \in \mathrm{Obj}(\mathcal{C})$.
2. Vector spaces over a field k form a category Vect_k with morphisms being linear maps; groups form a category Grp with morphisms being group homomorphisms; similarly abelian groups form a category Ab (which is a (*full*) *subcategory* of Grp, just like the category FSet of finite sets is a full subcategory of Set); topological spaces form a category Top with morphisms being continuous maps. Thus, when we talk about "isomorphisms of topological spaces", we mean homeomorphisms.
3. An example of a category which will appear many times in this report is the category of sets equipped with a group action. Let G be a group acting on sets X and Y; the morphisms in this category are exactly the set-functions ϕ which make the diagram

$$\begin{array}{ccc} X & \xrightarrow{g} & X \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ Y & \xrightarrow{g} & Y \end{array}$$

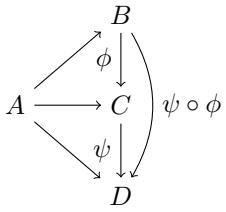
commute for all $g \in G$.
4. Let $\mathcal{C}$ be any category, and fix an object A. We can create a new category $\mathcal{C}^A$ whose objects are the elements of the sets $\mathrm{Hom}_{\mathcal{C}}(A, B)$ as B ranges over $\mathrm{Obj}(\mathcal{C})$, i.e. all morphisms in $\mathcal{C}$ starting at A. To remember this notation, consider the similarity between $\mathcal{C}^A$ and the notation $B^A = \{\text{set-functions } f : A \to B\}$. The morphisms in $\mathcal{C}^A$ are commutative diagrams

$$\begin{array}{ccc} & \overset{\phi}{\nearrow} & B \\ A & & \downarrow{\scriptstyle\chi} \\ & \underset{\psi}{\searrow} & C \end{array} .$$

To spell this out completely, $\mathrm{Hom}_{\mathcal{C}^A}(\phi, \psi) = \{\chi \in \mathrm{Hom}_{\mathcal{C}}(B, C) \mid \chi \circ \phi = \psi\}$, where $\phi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and $\psi \in \mathrm{Hom}_{\mathcal{C}}(A, C)$. Note here that we use the composition rule for morphisms in $\mathcal{C}$. This really is a category: the identity elements are

$$\begin{array}{ccc} & \overset{\phi}{\nearrow} & B \\ A & & \downarrow{\scriptstyle \mathrm{Id}_B} \\ & \underset{\phi}{\searrow} & B \end{array}$$

and composition is well-defined:



.

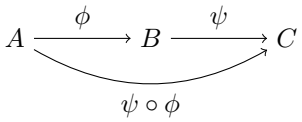
Here $\psi \circ \phi \in \mathrm{Hom}_{\mathcal{C}}(B, D)$ because $\mathcal{C}$ is a category. Finally, associativity of composition of morphisms in $\mathcal{C}^A$ follows in a similar manner from associativity of composition in $\mathcal{C}$.
An analogous category is $\mathcal{C}_A$, whose objects are the morphisms in the sets $\mathrm{Hom}_{\mathcal{C}}(B, A)$ as B ranges over $\mathrm{Obj}(\mathcal{C})$. ⧫

2.2 Functors

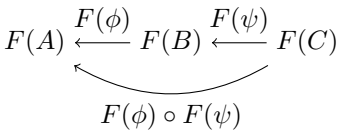
Categories give us a convenient way of studying structures in general, and it is natural to ask if we can also construct a category of categories. In order to do so, we have to define a proper notion of morphisms between categories; these do exist, and are called functors.

Definition 2.3. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be categories. A *(covariant) functor* F from $\mathcal{C}_1$ to $\mathcal{C}_2$ is a rule which sends any object A in $\mathrm{Obj}(\mathcal{C}_1)$ to an associated object $F(A)$ in $\mathrm{Obj}(\mathcal{C}_2)$ and any morphism $\phi \in \mathrm{Hom}_{\mathcal{C}_1}(A, B)$ to an associated morphism $F(\phi) \in \mathrm{Hom}_{\mathcal{C}_2}(F(A), F(B))$, in such a way that $F(\mathrm{Id}_A) = \mathrm{Id}_{F(A)}$ and $F(\phi \circ \psi) = F(\phi) \circ F(\psi)$.
Moreover, we say that F is *fully faithful* if each of the maps $\mathrm{Hom}_{\mathcal{C}_1}(A, B) \to \mathrm{Hom}_{\mathcal{C}_2}(F(A), F(B))$ is a bijection. We say F is *essentially surjective* if for each X in $\mathrm{Obj}(\mathcal{C}_2)$, there exists Y in $\mathrm{Obj}(\mathcal{C}_1)$ such that $F(Y)$ is isomorphic to X.

Given a category $\mathcal{C}$, it is easy to check that we can define a category $\mathcal{C}^{\mathrm{op}}$ whose objects are the objects of $\mathcal{C}$ and for which we set $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B) := \mathrm{Hom}_{\mathcal{C}}(B, A)$. A functor from $\mathcal{C}_1$ to $\mathcal{C}_2^{\mathrm{op}}$ is also called a *contravariant functor* from $\mathcal{C}_1$ to $\mathcal{C}_2$. Note that contravariant functors switch the order of composition: $F(\psi \circ \phi) = F(\phi) \circ F(\psi)$: the commutative diagram



gets sent to

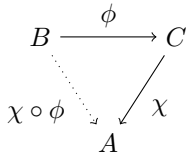


.

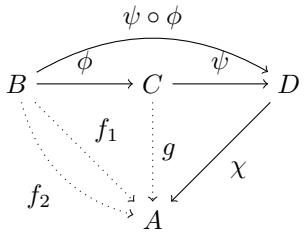
Examples 2.4.
1. A trivial example of a functor is the identity functor $\mathrm{Id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$. Closely related to this are so-called *forgetful functors*. A field, for example, comes with an additive and multiplicative group structure. Thus, we can define two functors from the category Field of fields to the category Ab of abelian groups. Say F_+ sends any field to its additive group, and $F_\times$ sends any field to its

multiplicative group. These functors are both forgetful, but they are not the same; e.g. the trivial group is in the image of $F_\times$, but not in the image of F_+. Still, both F_+ and $F_\times$ act like the identity on morphisms, as any morphism of fields is a fortiori a morphism of abelian groups; but for this reason, forgetful functors will rarely be fully faithful. F_+ also acts like the identity on the objects of Field. Forgetful functors obtain their name because they "forget" about part of the structure in the domain category.

2. Given any category $\mathcal{C}$ and any object A in $\mathrm{Obj}(\mathcal{C})$, we have a covariant functor $\mathrm{Hom}_\mathcal{C}(A, \bullet)$ and a contravariant functor $\mathrm{Hom}_\mathcal{C}(\bullet, A)$, both from $\mathcal{C}$ to Set. To see how morphisms are defined, let's have a closer look at the contravariant variant. Suppose we have a morphism $\phi \in \mathrm{Hom}_\mathcal{C}(B, C)$. Given $\chi \in \mathrm{Hom}_\mathcal{C}(C, A)$, ϕ induces a commutative diagram:



Writing $F = \mathrm{Hom}_\mathcal{C}(\bullet, A)$, we see that it is natural to set $F(\phi) = \phi^* \in \mathrm{Hom}_\mathsf{Set}(F(C), F(B))$, as it is a set-function sending any morphism in $F(C)$ to a morphism in $F(B)$. Note that F is then indeed contravariant. Composition works accordingly: consider the diagram



This diagram commutes. Indeed, $f_1 = g \circ \phi = (\chi \circ \psi) \circ \phi = \chi \circ (\psi \circ \phi) = f_2$. This shows that $F(\psi \circ \phi) = F(\phi) \circ F(\psi)$, as required.

3. Another relevant example of a contravariant functor is $\mathrm{Gal}_k(\bullet)$, which takes any Galois field extension K of a field k to its group of k-automorphisms. The fundamental theorem of Galois theory says that intermediate fields $K/F/k$ correspond to subgroups of $\mathrm{Gal}_k(K)$. Suppose K and F are both Galois over k. Then we have an embedding $F \hookrightarrow K$, giving rise to a group homomorphism $\mathrm{Gal}_k(K) \to \mathrm{Gal}_k(F)$ given by restriction of the field automorphisms of K to F. This duality is compatible with composition, so is indeed a functor. Unfortunately, we miss out on a lot of interesting behaviour by only restricting our attention to Galois extensions of k; towards the end of the report, we will see a more sophisticated version of this functor. ⧫

2.3 Natural transformations

We can go one step further and consider all functors mapping between two fixed categories. It turns out that these form a category in their own right, which is a very interesting object of study. Let's first define morphisms for such functor categories.

Definition 2.5. Suppose F and G are functors from $\mathcal{C}_1$ to $\mathcal{C}_2$. Let Φ be a collection of morphisms $\Phi_A \in \mathrm{Hom}_{\mathcal{C}_2}(F(A), G(A))$, one for each object A of $\mathcal{C}_1$. We say Φ is a *morphism of functors* or

natural transformation if for all A, B in $\mathrm{Obj}(\mathcal{C}_1)$ and all ϕ in $\mathrm{Hom}_{\mathcal{C}_1}(A, B)$, the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{\Phi_A} & G(A) \\ {\scriptstyle F(\phi)}\downarrow & & \downarrow{\scriptstyle G(\phi)} \\ F(B) & \xrightarrow{\Phi_B} & G(B) \end{array}$$

commutes.

We ought to check that this really turns functors from $\mathcal{C}_1$ to $\mathcal{C}_2$ into a category. Let F, G, H be functors, and Φ and Ψ be morphisms of functors from F to G, G to H, respectively. We can define the composition $\Phi \circ \Psi$ to be the collection of morphisms $\Phi_A \circ \Psi_A$, which is well-defined in $\mathcal{C}_2$. Associativity then follows immediately from associativity of morphisms in $\mathcal{C}_2$. Moreover, with this definition it is clear that $\mathrm{Id}_F : F \to F$, the morphism of functors consisting of the identity morphisms $\mathrm{Id}_{F(A)}$ for each A in $\mathrm{Obj}(\mathcal{C}_1)$, satisfies the properties of the identity morphism.
The notion of a natural transformation is important because it allows us to make precise analogies between different categories, which is one of the main purposes of this report. The following definition is key:

Definition 2.6. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be categories. If there exist functors F from $\mathcal{C}_1$ to $\mathcal{C}_2$ and G from $\mathcal{C}_2$ to $\mathcal{C}_1$ and isomorphisms of functors $\Phi : G \circ F \to \mathrm{Id}_{\mathcal{C}_1}$, $\Psi : F \circ G \to \mathrm{Id}_{\mathcal{C}_2}$, we say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are *equivalent* and F is an *equivalence*. If $\mathcal{C}_1$ is equivalent to $\mathcal{C}_2^{\mathrm{op}}$, we say $\mathcal{C}_1$ and $\mathcal{C}_2$ are *anti-equivalent*.

Having defined composition of morphisms of functors, it's an easy exercise to check that the above definition of equivalence is an equivalence relation on categories (as long as one ignores that categories don't form a set).
We will use the following lemma several times throughout this report; a proof can be found in [16, 1.4].

Lemma 2.7. Let $F : \mathcal{C}_1 \to \mathcal{C}_2$ be a functor. Then F is an equivalence if and only if F is fully faithful and essentially surjective.

Let us demonstrate the above by giving some concrete examples of equivalent categories.

Examples 2.8.
1. We saw in Example 2.2.4 that given a category $\mathcal{C}$ and an object A in $\mathcal{C}$, we can form the categories $\mathcal{C}_A$ and $\mathcal{C}^A$ of morphisms to and from A, respectively. Consider the categories $\mathsf{Set}^{\emptyset}$ and $\mathsf{Set}_{\{\emptyset\}}$. These are anti-equivalent.
To prove this claim, we need to construct a covariant functor $F : \mathsf{Set}^{\emptyset} \to \mathsf{Set}_{\{\emptyset\}}^{\mathrm{op}}$. Now luckily, this is not too difficult. The reason for this is that for each set S, there is exactly one morphism of sets $f_S : \emptyset \to S$ (the empty function), and also exactly one morphism of sets $g_S : S \to \{\emptyset\}$ (given by $s \mapsto \emptyset$ for all $s \in S$). It makes sense to set $F(f_S) = g_S$ for each S in $\mathrm{Obj}(\mathsf{Set})$.
What about morphisms? Using the above notation, suppose we have two distinct objects f_A and f_B in $\mathsf{Set}^{\emptyset}$. The morphisms from f_A to f_B are exactly the morphisms ϕ in $\mathrm{Hom}_{\mathsf{Set}}(A, B)$ such that $\phi \circ f_A = f_B$; but this is the case for *any* such ϕ. Thus, $\mathrm{Hom}_{\mathsf{Set}^{\emptyset}}(f_A, f_B) = \mathrm{Hom}_{\mathsf{Set}}(A, B)$. In a similar fashion, morphisms in $\mathsf{Set}_{\{\emptyset\}}$ from g_A to g_B are those set-functions $\psi : B \to A$ such that $g_A \circ \psi = g_B$; i.e. $\mathrm{Hom}_{\mathsf{Set}_{\{\emptyset\}}}(g_A, g_B) = \mathrm{Hom}_{\mathsf{Set}}(B, A)$; i.e. $\mathrm{Hom}_{\mathsf{Set}^{\emptyset}}(f_A, f_B) = \mathrm{Hom}_{\mathsf{Set}_{\{\emptyset\}}^{\mathrm{op}}}(F(f_A), F(f_B))$. Comparing these two descriptions, we see that we can let F be the

identity on morphisms; then any $\phi : f_A \to f_B$ gives a morphism $F(\phi) : g_B \to g_A$. This manifestly preserves identities and composition in the way of covariant functors, so F is indeed a functor. From this description of F, we can easily construct an inverse functor G: it sends g_S to f_S and is the identity on morphisms. Now $F \circ G = \mathrm{Id}_{\mathsf{Set}^{\mathrm{op}}_{\{\emptyset\}}}$ and $G \circ F = \mathrm{Id}_{\mathsf{Set}^{\emptyset}}$, which is what we wanted to show. (In fact, we have shown that the above categories are isomorphic, which is a stronger property than being equivalent; note that the definition of equivalence of functors only requires us to find functors which are mutually inverse *up to isomorphism of functors*, whereas here we have found two functors which really are mutually inverse.)

2. Here is an example of two categories which are clearly non-isomorphic, but still equivalent. Let $\mathcal{C}$ be a category whose objects are $\emptyset$ and the sets $\{1, \ldots, n\}$ for each $n \geq 1$, and whose morphisms are set-functions. Then $\mathcal{C}$ is equivalent to FSet. Indeed, the inclusion functor is certainly fully faithful, as $\mathrm{Hom}_{\mathcal{C}}(A, B) = \mathrm{Hom}_{\mathsf{FSet}}(A, B)$ for any two objects A, B of $\mathcal{C}$. It is also essentially surjective, as any finite set is either empty or bijective to a set of n elements for some $n \geq 1$.

3. Let k be an algebraically closed field. Let Aff_k denote the category of affine varieties (zero-loci of finite lists of polynomials over k), with morphisms given by regular maps, and let RFAlg_k denote the category of reduced, finitely-generated k-algebras. The functor F which sends an affine variety V to its coordinate ring $k[V]$ and a morphism $\phi : V \to W$ to $F(\phi) = \phi^* : k[W] \to k[V]$ is an anti-equivalence between Aff_k and RFAlg_k.

We first show that F is fully faithful. To do this, we show that $\phi \mapsto \phi^*$ has an inverse: let $W \subseteq \mathbb{A}^n_k$. Then given a k-algebra homomorphism $g : k[W] \to k[V]$, we can construct a regular map $(g(X_1), \ldots, g(X_n))$; in the case $g = \phi^*$, this regular map is exactly ϕ.

Next, we show that any reduced, finitely-generated k-algebra A is isomorphic to some $k[V]$. Let A be generated by $a_1, \ldots, a_n$. Define a k-algebra homomorphism $\alpha : k[X_1, \ldots, X_n] \to A$ by mapping $X_i \mapsto a_i$. α is surjective because the a_i generate A; hence, $k[X_1, \ldots, X_n]/\ker(\alpha) \cong A$. Since A is reduced, $\ker(\alpha)$ is a radical ideal in $k[X_1, \ldots, X_n]$; indeed, if $f \notin \ker(\alpha)$ but $f^m \in \ker(\alpha)$ for some $m \in \mathbb{N}_{>0}$, then $[f]$ would be a non-zero nilpotent in A. Thus, if we set $V := \mathbb{V}(\ker(\alpha)) \subseteq \mathbb{A}^n_k$, then $\ker(\alpha) = \mathbb{I}(V)$ by Hilbert's Nullstellensatz; and since $k[V]$ is the quotient of the polynomial ring by the ideal vanishing on V, this shows that $A \cong k[V]$. (Here we use the notation $\mathbb{V}(I) = \{\bar{x} \in \mathbb{A}^n_k \mid f(\bar{x}) = 0 \ \forall f \in I\}$ and $\mathbb{I}(V) = \{f \in k[X_1, \ldots, X_n] \mid f(\bar{x}) = 0 \ \forall \bar{x} \in V\}$. The Nullstellensatz states that $\mathbb{I}(\mathbb{V}(I)) = \mathrm{rad}(I)$ for any ideal I of $k[X_1, \ldots, X_n]$.) ♦

2.4 Universal Properties

If we can prove a statement about categories in general, we will at once prove this statement for many different structures. Of course, very little can be proven in complete generality, because the requirements to form a category are very weak. However, if we make some further assumptions on the category we are working with, we can prove some interesting things for a big class of structures; similarly, we can say things about the properties of categories which have certain kinds of objects, without assuming the existence of said objects. Many of these results take the form of *universal properties*. Loosely said, something satisfies a universal property in a category if it is the unique object (up to isomorphism) fitting inside a certain commutative diagram.

If we can find objects in different categories which satisfy the same universal property, in a sense this means that they play the same role in the category. Thus, universal properties are a useful tool for finding similarities between categories.

Definition 2.9. Let $\mathcal{C}$ be a category. We say an object A of $\mathcal{C}$ is *terminal* if one of the following holds:

1. For any object B of $\mathcal{C}$, $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is a singleton;

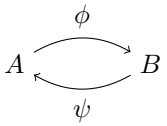
2. For any object B of $\mathcal{C}$, $\mathrm{Hom}_{\mathcal{C}}(B, A)$ is a singleton.

Terminal objects are sometimes referred to more specifically as *initial objects* if they satisfy property 1, or *final objects* if they satisfy property 2.

In Example 2.8.1, we have seen that the initial object in Set is the empty set. Set also has terminal objects: any singleton will do. Note that there are many different singletons; in fact they form a proper class, as $\{A\}$ is a singleton for any set A. However, any two singletons are isomorphic. This generalizes: categories need not have terminal objects, but if they exist, they have a strong uniqueness property:

Proposition 2.10. Terminal objects are unique up to unique isomorphism.

Proof. Suppose A is an initial object in $\mathcal{C}$. Applying the definition to $\mathrm{Hom}_{\mathcal{C}}(A, A)$, we see that the unique morphism from A to itself is Id_A.
Now suppose B is another initial object in $\mathcal{C}$; then the above also shows that $\mathrm{Hom}_{\mathcal{C}}(B, B) = \{\mathrm{Id}_B\}$. We know that there exists a unique morphism from A to B and a unique morphism from B to A:



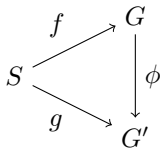
By the composition axiom for morphisms, we have $\psi \circ \phi \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ and $\phi \circ \psi \in \mathrm{Hom}_{\mathcal{C}}(B, B)$. This forces $\psi \circ \phi = \mathrm{Id}_A$, $\phi \circ \psi = \mathrm{Id}_B$. Thus, there is a unique isomorphism $\phi : A \xrightarrow{\sim} B$.
The proof for final objects is entirely similar. □

Definition 2.11. Let $\mathcal{C}$ be a category. We say A in $\mathrm{Obj}(\mathcal{C})$ *satisfies a universal property* if A is terminal in $\mathcal{C}$.

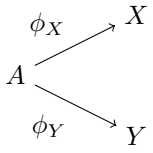
Note that Proposition 2.10 immediately shows us that any object satisfying a universal property is unique up to unique isomorphism. This is what makes universal properties a very powerful notion.

The above definition is vague and does not entirely capture the meaning of universal properties until one has seen some examples, the reason being that the category $\mathcal{C}$ may a priori seem somewhat obscure. In general, objects that satisfy a universal property are often objects (in another category) equipped with certain morphisms, and the universal property describes what conditions this combination fulfills. In order to make sense of this, let us look at some examples.

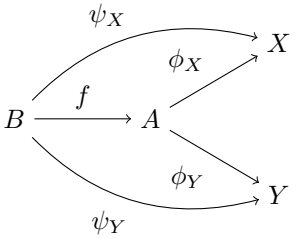
Examples 2.12.
1. Free groups are an example of an object satisfying a universal property. It can be stated as follows: let S be a set. Then the free group F_S on S, endowed with the inclusion $\iota : S \hookrightarrow F_S$, is universal with respect to the property that for any group G and set-function $f : S \to G$, there exists a unique group homomorphism $\phi : F_S \to G$ such that $\phi \circ \iota = f$.
This works because given a set S, we can create a category $\mathcal{C}$ in which the objects are set-functions $S \to G$, where G is any group. If $f : S \to G$ and $g : S \to G'$ are two objects, we can define $\mathrm{Hom}_{\mathcal{C}}(f, g)$ to be the set of group homomorphisms $\phi : G \to G'$ such that the triangle



commutes. It should not be mysterious by now that $\mathcal{C}$ really is a category, i.e. that we have identity morphisms and a composition law which satisfies the axioms.
Now it is easy to see that the free group on S is an initial object in $\mathcal{C}$. This not only shows that the given universal property is well-defined, but also that, given a set S, the free group on S is unique up to unique isomorphism.
2. We now come back to the motivating example we started the section with. We mentioned that in Set, the Cartesian product $X \times Y$ along with the projections π_X and π_Y satisfies a universal property, namely the following: for any set Z and functions $f : Z \to X$, $g : Z \to Y$, there exists a unique function $h : Z \to X \times Y$ such that $f = \pi_X \circ h$ and $g = \pi_Y \circ h$. How does this fit in with the above definition of universal properties?
The observation we need here is that we can form a category $\mathsf{Set}_{X,Y}$ in which the objects are diagrams



where A is any set and ϕ_X, ϕ_Y are functions; equivalently one can think of objects as being triplets (A, ϕ_X, ϕ_Y). The morphisms correspond to functions f which induce commutative diagrams



.

Again, at this point there should be no confusion that this construction does give a category; there really is only one sensible way in which to define composition.
Our previous discussion of this example tells us exactly that $(X \times Y, \pi_X, \pi_Y)$ is a final object in $\mathsf{Set}_{X,Y}$. Thus, the direct product satisfies the universal property, and any other set which also satisfies it must be in bijection with it.
Objects satisfying the above universal property are called *products*. The dual notion is that of *coproducts*, which we will enounter later, and the meaning of which the reader may for now ponder at their own leasure. (*Hint*: in the category of sets, the coproduct of X and Y is given by $X \sqcup Y$.) ⧫

2.5 Monomorphisms and epimorphisms

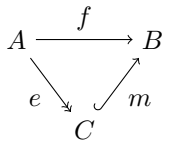
When talking about set-functions, we distinguish between different kinds of functions; in particular, injective and surjective functions play an important role. The following definitions generalise these notions.

Definition 2.13. Let $\mathcal{C}$ be a category. We say a morphism $\phi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ is a *monomorphism* if for any object Z and morphisms $f, g \in \mathrm{Hom}_{\mathcal{C}}(Z, A)$, $\phi \circ f = \phi \circ g \implies f = g$.
We call ϕ an *epimorphism* if for any object Z and morphisms $f, g \in \mathrm{Hom}_{\mathcal{C}}(B, Z)$, $f \circ \phi = g \circ \phi \implies f = g$.

Note that for set-functions, monomorphisms are exactly the injective functions, and epimorphisms are the surjective functions. We have the following easy proposition:

Proposition 2.14. Any set-function f can be written as $f = m \circ e$, where m is a monomorphism and e is an epimorphism.

Proof. Let $f \in \mathrm{Hom}_{\mathsf{Set}}(A, B)$, and consider the set $C = \mathrm{Im}(f)$. We want the following diagram to commute:



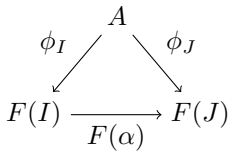
It is enough to set $e(a) = f(a)$ for all $a \in A$ and let m be the inclusion. Now e is surjective by the choice of C, and m is clearly injective; finally, $(m \circ e)(a) = f(a)$ by construction. □

The above proposition almost does not seem worth proving, but it is good to realise that set-functions have this property. This will become clearer when we talk about Galois categories.

2.6 Limits and colimits

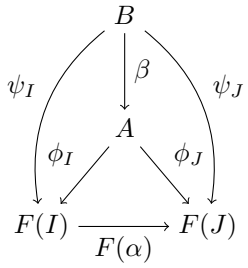
We will now turn our attention to two very important constructions in category theory: categorical limits and colimits. As the names suggest, the two are related and 'dual' to each other. In the following, the category $\mathcal{I}$ we will work with can best be thought of as an ordered indexing set, where there exists a morphism between objects I_1 and I_2 if and only if $I_1 \leq I_2$. This analogy works because the ordering $\leq$ is reflexive and transitive, giving us identity morphisms and enabling us to compose morphisms.

Definition 2.15. Let $\mathcal{I}$ and $\mathcal{C}$ be categories, and $F : \mathcal{I} \to \mathcal{C}$ a covariant functor. An object A in $\mathcal{C}$, equipped with morphisms $\phi_I : A \to F(I)$ for each object $I \in \mathcal{I}$, is called a *cone* for F if for any two objects I and J in $\mathcal{I}$ and morphism $\alpha : I \to J$, the diagram



commutes.

It's easily checked that cones for F form a category: if (A, ϕ) and (B, ψ) are both cones for F, the morphisms between them are just morphisms $\beta \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ such that all diagrams

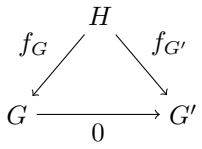


commute.

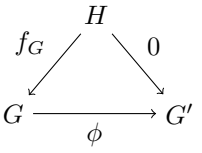
Definition 2.16. Let L be a final object in the category of cones for F, provided this exists. Then we call L the *limit* of F, denoted $\varprojlim F$. We say the limit is *finite* if $\mathrm{Obj}(\mathcal{I})$ is finite and $\mathrm{Hom}_{\mathcal{I}}(I, J)$ is finite for all $I, J \in \mathrm{Obj}(\mathcal{I})$.

Limits generalise many notions we are already familiar with, as we will demonstrate now.

Examples 2.17.
1. Let $\mathcal{I}$ be the empty category and $F : \mathcal{I} \to \mathcal{C}$ the empty functor. The existence of $\varprojlim F$ is then equivalent to the existence of a final object in $\mathcal{C}$.
2. We have previously defined what products are: if $\mathcal{C}$ is a category and A and B are objects, their product is the final object in the category $\mathcal{C}_{A,B}$ of morphisms to A and B. But this is exactly the same as the limit of the functor F mapping from any category $\mathcal{I}$ with two objects, with the only morphisms being the identity morphisms, to $\mathcal{C}$, where $F(I_1) = A$ and $F(I_2) = B$. We call a category like $\mathcal{I}$, in which the only morphisms are identity morphisms, *discrete*.
Similarly, we can define the product of any collection of objects $\{A_i\}_{i \in I}$ of $\mathcal{C}$ by taking F to be the functor mapping from a discrete category $\mathcal{I}$ to $\mathcal{C}$, where $\mathrm{Obj}(\mathcal{I}) = I$ and $F(I_i) = A_i$. However, one should again keep in mind that products need not always exist.
3. Consider the category $\mathcal{I}$, where $\mathrm{Obj}(\mathcal{I}) = \{I, J\}$, and besides the identity morphisms, there are two morphisms α and β mapping from I to J. Let F be a functor from $\mathcal{I}$ to Grp such that $F(I) = G$, $F(J) = G'$, $F(\alpha) = \phi \in \mathrm{Hom}_{\mathsf{Grp}}(G, G')$, and $F(\beta)$ is the zero map from G to G'. What will $\varprojlim F$ be in this case?
Well, if there is a group H which is the limit of F, we need the following diagram to commute:



Thus, $f_{G'}$ must be the zero function. Using this information in the second diagram



,

we see that for this to commute, we need $f_G(H) \subseteq \ker(\phi)$. In fact, if we set $H = \ker(\phi)$ and let f_G be the inclusion, it's not hard to see that this satisfies the properties of a limit for F: if H' is a cone for F, then the morphism $H' \to G'$ must be the zero map, and since $g_G(H') \subseteq \ker(\phi)$, $g_G : H' \to G$ factors uniquely through $\ker(\phi)$ as $g_G = f_G \circ \gamma$. This γ is the unique morphism of cones for F (from H' to $\ker(\phi)$) we were looking for.
4. Recall that a profinite group can be constructed from an inverse system of finite groups. We see now that this construction is just an instance of a limit in TGrp of topological groups, where the finite groups are endowed with the discrete topology. An interesting application is the *profinite completion* $\hat{G}$ of a group G, which is by definition the inverse limit over its finite quotients. If N_i and N_j are normal subgroups of G, we say $i \geq j \iff N_i \subseteq N_j$, in which case we take $\phi_{ij} : G/N_i \to G/N_j$ to be the natural homomorphism.
We see straight away that the profinite completion of a finite group is isomorphic to itself: finite groups have finitely many finite quotients, so in this case $\hat{G}$ consists of finite sequences

$(g_n, g_{n-1}, \ldots, g_1)$. Now the fact that these sequences must be compatible with the natural maps between the quotients mean that they are determined by the element $g_n \in G = G/\{e\}$. Indeed, we have $n \geq i$ for any i (as any normal subgroup contains the identity element), and so knowing g_n determines $g_i = \phi_{ni}(g_n)$ for all i.

5. Things get more interesting when we consider infinite groups. For instance, take the additive group $\mathbb{Z}$. It is abelian, so any subgroup is normal, and so its finite quotients are $\mathbb{Z}/n\mathbb{Z}$ for any $n \geq 1$. $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m \mid n$, so the ordering is given by divisibility. What we get is that $\hat{\mathbb{Z}}$ consists of sequences of integers $(\ldots, a_n, \ldots, a_2, a_1)$ with $0 \leq a_i < i$, such that $a_n \equiv a_m \pmod{m}$ whenever $m \mid n$.

Note that $\mathbb{Z}$ embeds into its profinite completion in a natural way: there is an injective homomorphism $\mathbb{Z} \to \hat{\mathbb{Z}}$ sending n to the sequence $([n]_m)_{m \in \mathbb{Z}}$ where $[n]_m$ is the image of n in $\mathbb{Z}/m\mathbb{Z}$. It is tempting to hope that any group embeds into its profinite completion, but this is not the case. For instance, infinite simple groups (e.g. $PSL_2(\mathbb{R})$) have only one finite quotient, which is the quotient by itself; thus, its profinite completion is trivial. More generally, a group embeds into its profinite completion if and only if it is *residually finite* (see [10] for details).

6. We can construct more profinite groups starting from $\mathbb{Z}$ if we look at different systems of subgroups. For example, we can obtain the p-adic integers $\mathbb{Z}_p$ for any prime number p by only considering the subgroups of the form $p^n\mathbb{Z}$; since $p^m \mid p^n$ for any $n \geq m$, the ordering is the usual one. Hence, $\mathbb{Z}_p$ can be described as

$$\mathbb{Z}_p = \{(\ldots, g_n, \ldots, g_2, g_1, g_0) \mid g_k \in \mathbb{Z}/p^k\mathbb{Z} \text{ and } g_i \equiv g_j \pmod{p^j} \text{ whenever } i \geq j\},$$

or equivalently,

$$\mathbb{Z}_p = \{(\ldots, h_n, \ldots, h_2, h_1) \mid 0 \leq h_i < p\},$$

where an isomorphism from the second to the first set is given by

$$(\ldots, h_n, \ldots, h_2, h_1) \longmapsto (\ldots, \sum_{i=1}^{n} h_i p^i, \ldots, h_2 p + h_1, h_1, 0).$$

The second description allows us to write a p-adic integer x as $x = \ldots x_3 x_2 x_1$, where $0 \leq x_i < p$, where the x_i are called the *digits* of x. There are reasons why it is convenient to view $\mathbb{Z}_p$ as numbers with a decimal expansion: we can do arithmetic with them as with usual integers, and under the p-adic norm, the digits on the left "contribute the least". This is analogous to writing usual numbers as, e.g., $\pi = 3.14\ldots$, as under the Euclidean norm, the further to the right we go, the smaller the contributions of the digits get. These properties are more interesting when studying the p-adics from an analytic, rather than an algebraic, point of view, so although this is an interesting subject, we don't have to worry about it here. ⧫

An additional convenience is that limits satisfy a universal property by definition; thus, if we can express an object as a limit of some functor, we know it is unique up to unique isomorphism. It is important to realise that the category $\mathcal{I}$ can be more complicated than in the examples we've seen so far. For instance, later on we will see examples of limits where $\mathcal{I}$ is infinite.

The reader who has internalised the notion of limit will now see that the colimit is a very similar notion indeed.

Definition 2.18. Let $\mathcal{I}$ and $\mathcal{C}$ be categories as before, and $F : \mathcal{I} \to \mathcal{C}$ a covariant functor. A

co-cone of F is an object A of $\mathcal{C}$ equipped with morphisms $\phi_I : F(I) \to A$ such that all diagrams

$$\begin{array}{ccc} F(I) & \xrightarrow{F(\alpha)} & F(J) \\ & {\scriptstyle \phi_I} \searrow \quad \swarrow {\scriptstyle \phi_J} & \\ & A & \end{array}$$

commute. The initial object in the category of co-cones of F, if it exists, is called the *colimit* of F, denoted $\varinjlim F$. We say the colimit is *finite* if $\mathrm{Obj}(\mathcal{I})$ is finite and $\mathrm{Hom}_{\mathcal{I}}(I, J)$ is finite for all $I, J \in \mathrm{Obj}(\mathcal{I})$.

The terminology *inverse limit* or *projective limit* is also used to denote limits; similarly, one may refer to a colimit as a *direct limit* or *injective limit*. It should be clear that many of the manifestations of limits we have seen have corresponding manifestations as colimits; these are aptly called coproducts, cokernels, etc., some of which have been referred to before. Colimits will be just as important as limits in what follows (especially coproducts will appear often), so the reader is encouraged to ensure they understand these concepts fully before moving on.

2.7 Exactness

We need a few more notions before we can axiomatically introduce Galois categories. One of them is exactness of functors.

Definition 2.19. Suppose $F : \mathcal{C}_1 \to \mathcal{C}_2$ is a functor. We say F is *left-exact* if F commutes with limits, i.e. if $G : \mathcal{I} \to \mathcal{C}_1$ is a functor, then $F(\varprojlim G) = \varprojlim (F \circ G)$ whenever the first limit exists. We say F is *right-exact* if F commutes with colimits, and finally we say F is *exact* if it is both left-exact and right-exact.

The terminology stems from the fact that exact functors preserve exactness of sequences (in categories in which it makes sense to speak of these things); in fact, in such categories (called *abelian categories*, see e.g. [5]), these two conditions are equivalent. For example, consider the functor $F : \mathsf{Grp} \to \mathsf{Ab}$ which sends any group G to its abelianization G_{ab}, i.e. the quotient of G by its commutator subgroup; any morphism of groups $\phi : G \to H$ induces a morphism of abelian groups $\tilde{\phi} : G_{\mathrm{ab}} \to H_{\mathrm{ab}}$ by composition with the quotient map, so we let $F(\phi) = \tilde{\phi}$ be this induced homomorphism. In both Grp and Ab we can talk about exact sequences. Recall that a sequence

$$G_n \xrightarrow{\phi_n} G_{n-1} \xrightarrow{\phi_{n-1}} \cdots \xrightarrow{\phi_2} G_1 \xrightarrow{\phi_1} G_0$$

is called *exact* if $\mathrm{Im}(\phi_i) = \ker(\phi_{i-1})$ for each $1 < i \leq n$.
For F to be left-exact, we need any exact sequence

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C$$

to be sent to an exact sequence under F:

$$0 \longrightarrow F(A) \xrightarrow{F(\phi)} F(B) \xrightarrow{F(\psi)} F(C)$$

Similarly, F is right-exact if and only if F preserves exactness of

$$A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0 \ ,$$

and F is exact if and only if F sends short exact sequences to short exact sequences.
It is not very hard, but slightly tedious, to show that the functor F which maps groups to their abelianizations is right-exact but not left-exact. The diligent reader may want to prove this by themselves.

2.8 Subobjects

In many categories, it is useful to be able to talk about "subobjects", by which we mean things like subsets of sets, subgroups of groups, subrings of rings, etc. It turns out that there is a natural way to generalise this notion, and we have already developed the tools to do so.

Definition 2.20. A *subobject* of an object $A \in \mathrm{Obj}(\mathcal{C})$ is an isomorphism class of monomorphisms m with codomain A. Here two monomorphisms $m_1 : S_1 \to A$ and $m_2 : S_2 \to A$ are said to be isomorphic if and only if they factor through each other, i.e. there exist morphisms $f_1 : S_1 \to S_2$ and $f_2 : S_2 \to S_1$ such that $m_1 = m_2 \circ f_1$ and $m_2 = m_1 \circ f_2$.
Given a subobject $S \to A$, a *complement* is a second subobject $T \to A$ such that the induced morphism $S \sqcup T \to A$ is an isomorphism (where $S \sqcup T$ denotes the coproduct of S and T in $\mathcal{C}$).

The reason why we consider subobjects to be isomorphism classes of monomorphisms is because there would otherwise be too many subobjects for the notion we are trying to generalise. For example, a finite, non-empty set X should have exactly $2^{|X|}$ subobjects in Set. If we did not look at isomorphism classes, we would have infinitely many subobjects, as there is a monomorphism $S \to X$ for any singleton S. Quotienting out by the isomorphism relation in this case identifies all the functions from singletons which have the same image, and gives us exactly the notion we want.

3 Galois Categories

3.1 The axioms

We can now introduce the notion of a Galois category. Galois categories were introduced by Grothendieck in his SGA [6, exposé V.4]; the definition given here is the one appearing in [17].

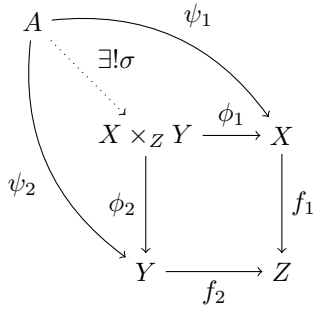
Definition 3.1. Let $\mathcal{C}$ be a category, and $F : \mathcal{C} \to \mathsf{FSet}$ a functor. We call the pair $(\mathcal{C}, F)$ a *Galois category* with *fundamental functor* F if the following axioms are satisfied:

1. All finite limits and colimits exist in $\mathcal{C}$;
2. F is conservative ($F(\phi)$ is an isomorphism only if ϕ is an isomorphism) and exact;
3. Any morphism decomposes as a composition of a monomorphism of an epimorphism;
4. Each subobject of $\mathcal{C}$ admits a complement.

Note that if $F : \mathcal{C}_1 \to \mathcal{C}_2$ is a functor, then F sends isomorphisms to isomorphisms: if $\phi \circ \psi = \mathrm{Id}_A$ and $\psi \circ \phi = \mathrm{Id}_B$, then (assuming F is covariant; the contravariant case is identical) by the properties of functors we have $F(\phi \circ \psi) = F(\phi) \circ F(\psi) = \mathrm{Id}_{F(A)}$ and $F(\psi \circ \phi) = F(\psi) \circ F(\phi) = \mathrm{Id}_{F(B)}$, so $F(\phi)$ and $F(\psi)$ are again mutually inverse isomorphisms. A functor is conservative if and only if the converse holds.

Suppose that we want to show that a certain category is Galois. At first sight, checking the first property is already problematic. How on earth would we go about showing that a category has *all* finite limits? We have seen that these include initial and final objects, products and coproducts, and much more. It seems an impossible task.

After thinking about this for a while, one may come up with a way of simplifying the problem by considering *fiber products*. Fiber products are just a special kind of limit, namely that of a functor $F : \mathcal{I} \to \mathcal{C}$ where $\mathrm{Obj}(\mathcal{I}) = \{I_1, I_2, I_3\}$ and the only non-trivial morphisms are $I_1 \to I_2$ and $I_3 \to I_2$: pictorially, it is the limit of a diagram $\bullet \to \bullet \leftarrow \bullet$. If the images of I_1, I_2 and I_3 are objects X, Z and Y, respectively, one denotes the fiber product $\varprojlim F$ by $X \times_Z Y$ (which of course implicitly depends on the accompanying morphisms). To summarise, the fiber product is the three-tuple $(X \times_Z Y, \phi_1, \phi_2)$ fitting into the following commutative diagram:



Lemma 3.2. If a category $\mathcal{C}$ has all fiber products and a final object, then $\mathcal{C}$ has all finite limits.

Proof. The first thing we note is that existence of fiber products and a final object implies existence of products: namely, if X denotes the final object, it follows straight from the definitions that $A \times_X B$ is just the product of A and B. We will denote the product by $A \times B$. Given maps

$\phi, \psi \in \mathrm{Hom}_{\mathcal{C}}(Z, A)$, we know that ϕ and ψ factor uniquely through the product $A \times A$, and as such we will denote this induced map by $\phi \times \psi$.
We now show that *equalizers* exist in $\mathcal{C}$: these are limits E of the form

$$\begin{array}{ccc} & E & \\ & \swarrow \quad \searrow & \\ A & \overset{a}{\underset{b}{\rightrightarrows}} & B \end{array} .$$

Note that the morphism $E \to B$ is determined by the morphism $E \to A$. For this reason, when talking about "the equalizer of a and b" we usually mean the morphism $E \to A$; if the morphism is clear from the context, we may also say E is the equalizer.
E can be constructed as follows. We first let $Z = A \times_B A$; then the equalizer is $E = Z \times_{A \times A} A$. More precisely, we have a fiber product

$$\begin{array}{ccc} Z & \xrightarrow{p_1} & A \\ {\scriptstyle p_2}\downarrow & & \downarrow{\scriptstyle b} \\ A & \xrightarrow[a]{} & B \end{array}$$

and using this, we construct

$$\begin{array}{ccc} E & \xrightarrow{\phi} & A \\ {\scriptstyle \psi}\downarrow & & \downarrow{\scriptstyle \mathrm{Id}_A \times \mathrm{Id}_A} \\ Z & \xrightarrow[p_1 \times p_2]{} & A \times A \end{array} .$$

Observe that E, along with the morphisms $b \circ p_1 \circ \psi : E \to B$ and $\phi \circ \mathrm{Id}_A = \phi : E \to A$ is indeed the equalizer: since $b \circ p_1 = a \circ p_2$ and $p_2 \circ \psi = \phi$, we have $b \circ p_1 \circ \psi = a \circ p_2 \circ \psi = a \circ \phi$, and since $p_1 \circ \psi = \phi$ we have $b \circ p_1 \circ \psi = b \circ \phi$. Next, E is final with respect to this property: if there is an object E' and morphisms $f : E \to A$ and $g : E \to B$ such that $a \circ f = b \circ f = g$, by finality of the fiber product we get a unique morphism $E' \to Z$, which then gives us (again by finality of the fiber product) a unique map $E' \to E$, as required.

So we have shown that if we have a final object and fiber products, we also have products (and by induction, finite products) and equalizers. The idea is now to use these instances of limits to create all other finite limits. We do this as follows. Let $F : \mathcal{I} \to \mathcal{C}$ be a functor, and let $\mathcal{I}$ have only finitely many morphisms. Let

$$P_1 = \prod_{I \in \mathrm{Obj}(\mathcal{I})} F(I); \qquad P_2 = \prod_{\substack{I,J \in \mathrm{Obj}(\mathcal{I}) \\ \phi : I \to J}} F(J).$$

We denote by $p_I : P_1 \to F(I)$ and $\pi_\phi : P_2 \to F(J)$ the projections from the respective products (where $\phi : I \to J$). The universal property of products says that a morphism $P_1 \to P_2$ is

uniquely determined by the morphisms from P_1 to each of the components of the product P_2. Thus, we can define morphisms ψ and χ from P_1 to P_2 as follows: for any morphism ϕ in $\mathcal{I}$, we let $\psi_\phi = \pi_\phi \circ \psi = p_{\mathrm{cod}(\phi)}$, and $\chi_\phi = \pi_\phi \circ \chi = F(\phi) \circ p_{\mathrm{dom}(\phi)}$. Now consider the equalizer

$$\begin{array}{ccc} & E & \\ {\scriptstyle\sigma}\swarrow & & \searrow \\ P_1 & \overset{\psi}{\underset{\chi}{\rightrightarrows}} & P_2 \end{array}.$$

E, equipped with the morphisms $\sigma_I = p_I \circ \sigma$, is the limit for F we were looking for. Indeed, any diagram

$$\begin{array}{ccc} & E & \\ {\scriptstyle p_I \circ \sigma}\swarrow & & \searrow{\scriptstyle p_J \circ \sigma} \\ F(I) & \xrightarrow[F(\phi)]{} & F(J) \end{array}$$

commutes because $F(\phi) \circ p_I \circ \sigma = F(\phi) \circ p_{\mathrm{dom}(\phi)} \circ \sigma = \chi_\phi \circ \sigma = \psi_\phi \circ \sigma = p_{\mathrm{cod}(\phi)} \circ \sigma = p_J \circ \sigma$; moreover, if we have any other cone E' for F, necessarily it will fit into a diagram

$$\begin{array}{ccc} & E' & \\ \swarrow & & \searrow \\ P_1 & \overset{\psi}{\underset{\chi}{\rightrightarrows}} & P_2 \end{array},$$

which means that there is a unique morphism $E' \to E$ of cones, as required. □

Dually, if $\mathcal{C}$ has all *fibered coproducts* (colimits of diagrams $\bullet \leftarrow \bullet \rightarrow \bullet$) and an initial object, then $\mathcal{C}$ has all finite colimits. Lemma 3.2 is very useful, not only for showing the existence of finite limits, but also for showing exactness: if a functor commutes with final objects and fiber products, then it commutes with all finite limits.

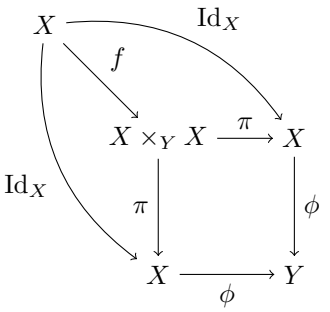
3.2 Properties

Because of the abstract definition, at first sight it is not clear why Galois categories are interesting objects of study. To motivate this, we will look at some key properties of Galois categories; we will use all of these later on, when proving the categorical Galois correspondence. From now on, $(\mathcal{C}, F)$ will be a Galois category, unless explicitly stated otherwise.

Lemma 3.3. $\phi \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ is a monomorphism (resp. epimorphism) if and only if $F(\phi) \in \mathrm{Hom}_{\mathsf{FSet}}(F(X), F(Y))$ is an injection (resp. surjection).

Proof. We prove the case where $\phi : X \to Y$ is a monomorphism; the case where ϕ is an epimorphism is proven identically by reversing all arrows.
The lemma follows from the following claim: $\phi : X \to Y$ is a monomorphism if and only if the unique morphism $f : X \to X \times_Y X$ which commutes with the identity morphisms is an isomorphism. Indeed, if this is true, then also $F(\phi) : F(X) \to F(Y)$ is an injection (a monomorphism in FSet) if and only if the unique morphism $F(f) : F(X) \to F(X) \times_{F(Y)} F(X)$ is an isomorphism, by exactness of F. Because F is conservative, this means that ϕ is a monomorphism if and only

if $F(\phi)$ is an injection, which is what we wanted.
So let's prove the claim. We know $\mathcal{C}$ has all finite limits, so in particular fiber products; thus we have an induced commutative diagram



where f is unique. First suppose ϕ is a monomorphism. Then $\phi \circ \pi \circ f = \phi \circ \mathrm{Id}_X$, so $\pi \circ f = \mathrm{Id}_X$. Now $\pi \circ f \circ \pi = \pi$, and therefore the morphism $f \circ \pi : X \times_Y X \to X \times_Y X$ is a morphism of cones. But so is $\mathrm{Id}_{X \times_Y X}$, and by the universal property of the fiber product, we have that $f \circ \pi = \mathrm{Id}_{X \times_Y X}$. Thus f is an isomorphism.

Conversely, suppose f is an isomorphism; then any morphism of cones $g : Z \to X \times_Y X$ yields a morphism of cones $f^{-1} \circ g : Z \to X$, which is unique: if $h : Z \to X$ was another such morphism, then $f \circ h : Z \to X \times_Y X$ is also a morphism of cones, so by the universal property of the fiber product we have $f \circ h = g$ and $h = f^{-1} \circ g$. What we've shown is that in fact, X (equipped with the identity morphisms) may itself be considered as the fiber product. But then if $\phi \circ a = \phi \circ b$, where a and b map from an object A, this means that (A, a, b) is a cone and so we have a unique morphism $\psi : A \to X$; commutativity of the diagram then tells us that $a = \psi = b$, i.e. ϕ is a monomorphism. □

One might wonder if the above lemma implies that the condition that F be conservative may be dropped. It seems plausible that conservativity of F is now implied by the fact that any morphism is a composition of a monomorphism of an epimorphism: if $\phi = m \circ e$ and $F(\phi)$ is an isomorphism, we can deduce that m and e are both monomorphisms as well as epimorphisms. However, these properties are not enough for ϕ to be an isomorphism in general: for example, a continuous bijection which is not a homeomorphism is both a monomorphism and an epimorphism in Top, but not an isomorphism.

The following definition ties in nicely with property 4 of Galois categories.

Definition 3.4. Let $\mathcal{C}$ be a category. We say an object X of $\mathcal{C}$ is *connected* if it has exactly two distinct subobjects.

Lemma 3.5. Any non-initial object in a Galois category can be written uniquely (up to reordering) as a finite coproduct of connected objects.

Proof. Let I denote the initial object in our Galois category. For any object X, we have the unique morphism $I \to X$ and the identity morphism $X \to X$. Because F is exact, $F(I) = \emptyset$, and the empty function is injective; moreover, the identity function $F(X) \to F(X)$ is a bijection. Thus, Lemma 3.3 tells us that the two given morphisms are actually subobjects, and it is easy to check that they are complements. Saying X is connected then amounts to saying that X has

no other subobjects than itself and I.

Now let X be any object such that $F(X)$ is a singleton (such X exists since $\mathcal{C}$ has final objects and F is conservative). As any decomposition of $F(X)$ into a coproduct (disjoint union) of two subobjects is of the form $F(X) \sqcup \emptyset$, X is connected and the statement holds for this case. Next, let X be such that $|F(X)| = n > 1$. If X is connected, we are done, so suppose it isn't; then we can write $X = Y \sqcup Z$, where neither Y nor Z are either I or X. By exactness, we have $F(X) = F(Y) \sqcup F(Z)$, and $0 < |F(Y)|, |F(Z)| < n$. By induction, we can write Y and Z as finite coproducts of connected objects, unique up to reordering, and so the same is true for X. □

Lemma 3.6. Any morphism $X \to Y$ in $\mathcal{C}$, where X is not the initial object and Y is connected, is an epimorphism.

Proof. We know the morphism $X \to Y$ factors as a composition $X \to Y' \to Y$ of a monomorphism of an epimorphism. Applying F, we get a diagram $F(X) \twoheadrightarrow F(Y') \hookrightarrow F(Y)$. $F(X)$ is non-empty as X is not initial, whence $F(Y')$ is non-empty; by connectedness of Y, this means that $Y' \to Y$ is an isomorphism and so $X \to Y$ was indeed an epimorphism. □

Corollary 3.7. Any morphism $X \to X$ of a connected object is an automorphism.

As an almost-converse to Lemma 3.6, we have the following:

Lemma 3.8. Let $e \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ be an epimorphism, where X is connected. Then Y is connected.

Proof. Suppose not. Let $m : Z \to Y$ be a subobject, where Z is neither initial nor isomorphic to Y. Fiber products exist in $\mathcal{C}$ and F is exact, so we obtain a commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{F(\pi_Z)} & F(Z) \\ {\scriptstyle F(\pi_X)}\downarrow & & \downarrow{\scriptstyle F(m)} \\ F(X) & \xrightarrow[F(e)]{} & F(Y) \end{array}.$$

We can explicitly describe $S = F(X) \times_{F(Y)} F(Z)$ as $\{(a, b) \in F(X) \times F(Z) \mid F(e)(a) = F(m)(b)\}$, $F(\pi_X)$ and $F(\pi_Z)$ being the restrictions to S of the projections onto either coordinate. Because $F(e)$ is surjective, for each $b \in F(Z)$ there exists at least one $a \in F(X)$ with $F(e)(a) = F(m)(b)$, and since $F(Z) \neq \emptyset$, this says that $S \neq \emptyset$. Similarly, because $F(m)$ is injective, for each $a \in F(X)$ there can be no more than one $b \in F(Z)$ with $F(e)(a) = F(m)(b)$, which says that $F(\pi_X)$ is injective; by Lemma 3.3, π_X is a subobject. By connectedness of X, π_X must be an isomorphism, and so for each $a \in F(X)$ there exists a unique $b \in F(Z)$ with $F(e)(a) = F(m)(b)$. It follows that $F(m)$ is in fact surjective, thus an isomorphism. Hence m is an isomorphism, but this contradicts our assumption. □

Proposition 3.9. $\mathrm{Aut}(X)$ is finite for each object X of $\mathcal{C}$. If X is connected, $|\mathrm{Aut}(X)| \leq |F(X)|$.

Proof. Assume first that X is connected, and let Y be any object of $\mathcal{C}$. We will show that $|\mathrm{Hom}_{\mathcal{C}}(X, Y)| \leq |F(Y)|$ by proving that the map

$$\begin{aligned} \mathrm{Hom}_{\mathcal{C}}(X, Y) &\longrightarrow F(Y) \\ \phi &\longmapsto F(\phi)(x), \end{aligned}$$

where $x \in F(X)$ is any fixed element, is injective. Indeed, suppose that $F(\phi)(x) = F(\psi)(x)$. We consider the equalizer

$$\begin{array}{ccc} & E & \\ & \swarrow \quad \searrow & \\ F(X) & \overset{F(\phi)}{\underset{F(\psi)}{\rightrightarrows}} & F(Y) \end{array} .$$

It is easily verified that $E = \{y \in F(X) \mid F(\phi)(y) = F(\psi)(y)\}$ and the map $E \hookrightarrow F(X)$ is the inclusion. Note that $x \in E$. Since F is exact, the above diagram must be the image under F of the equalizer of ϕ and ψ in $\mathcal{C}$; X is connected and this equalizer is a subobject by Lemma 3.3, and since $E \neq \emptyset$ it must be X itself. Thus $E = F(X)$ and $\phi = \psi$, which proves injectivity. The statement of the proposition follows by considering the case $Y = X$.
As for the general case: write $X = \coprod_{i=1}^{n} C_i$, where the C_i are connected objects. Any morphism $X \to Y$ uniquely determines morphisms $C_i \to Y$ for each i by composition with the canonical morphisms, and conversely, maps $C_i \to Y$ induce a unique map $X \to Y$ by the universal property of the coproduct; it follows that

$$|\mathrm{Hom}_{\mathcal{C}}(X, Y)| = \prod_{i=1}^{n} |\mathrm{Hom}_{\mathcal{C}}(C_i, Y)|.$$

Each of the terms in the product on the right is finite, so after setting $Y = X$, we are done. □

In the course of this proof we have also obtained the following useful result:

Corollary 3.10. Let $(\mathcal{C}, F)$ be a Galois category, X a connected object, and $\phi, \psi \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$. If $F(\phi)(x) = F(\psi)(x)$ for any $x \in F(X)$, then $\phi = \psi$.

3.3 Galois objects

Imagine for a second that $\mathcal{C}$ is a category like Set, where objects have elements and morphisms are functions. In this case, elements of $\mathrm{Aut}(X)$ act on X by permuting the elements of X, and we can look at the set of orbits under this action; if $G \leq \mathrm{Aut}(X)$, recall that the set of orbits is denoted X/G. We can generalise this notion to arbitrary categories: if $G \leq \mathrm{Aut}(X)$, we define X/G to be an object equipped with a morphism $p : X \to X/G$ such that $p \circ \sigma = p$ for each $\sigma \in G$, and which is initial with respect to this property; i.e. if $q : X \to Y$ satisfies $q \circ \sigma = q$ for all $\sigma \in G$, we have a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\quad q \quad} & Y \\ & {\scriptstyle p}\searrow \quad \nearrow {\scriptstyle \exists!\phi} & \\ & X/G & \end{array} .$$

This quotient need not always exist, but in Galois categories it does! This is because the above description says exactly that X/G is the co-equalizer of all $\sigma \in G$, and as we know, Galois categories have all finite colimits.

Definition 3.11. Let $(\mathcal{C}, F)$ be a Galois category, and let X in $\mathrm{Obj}(\mathcal{C})$ be connected. If $X/\mathrm{Aut}(X)$ is the final object, we say X is a *Galois object*.

Since F is exact, this is equivalent to saying $\mathrm{Aut}(X)$ acts transitively on $F(X)$, where the action is given by $(\phi, x) \mapsto F(\phi)(x)$. Indeed, the quotient $F(X)/G = F(X/G)$, where $G \leq \mathrm{Aut}(X)$, is just the set of orbits of $F(X)$ under the action of G.

Remark 3.12. By Proposition 3.9, if X is connected, $|\mathrm{Aut}(X)| \leq |F(X)|$; the reverse inequality holds for Galois objects by transitivity of the action, and so $|\mathrm{Aut}(X)| = |F(X)|$ for any Galois object X. Moreover, Corollary 3.10 says precisely that G acts freely on $F(X)$ for connected X.

Theorem 3.13. Any connected object is of the form X/G, where X is a Galois object and $G \leq \mathrm{Aut}(X)$.

Proof. Let Y be any object in $\mathcal{C}$, and write $Z = Y^{|F(Y)|}$ for the product of $|F(Y)|$ copies of Y (which exists because $\mathcal{C}$ has finite limits). It follows from exactness of F that $F(Z) = F(Y)^{|F(Y)|}$. Let $x \in F(Z)$ be the element whose y^{th} coordinate is y, for $y \in F(Y)$. Let X be the connected component of Z for which $x \in F(X)$.

Claim: X is a Galois object, and the map $\mathrm{Hom}_{\mathcal{C}}(X, Y) \to F(Y)$, $\phi \mapsto F(\phi)(x)$ is a bijection.

In the proof of Proposition 3.9, we showed that the above map is injective for connected X. Surjectivity follows easily from the above construction: if $y \in F(Y)$, let ϕ be the composition $X \to Z \to Y$, where $X \to Z$ is the subobject and $Z \to Y$ is the canonical morphism to the y^{th} coordinate. By exactness of F, $F(\phi)$ is exactly the "usual" projection onto the y^{th} coordinate of sets, so $F(\phi)(x) = y$. This shows the second part of the claim, and also allows us to characterize $\mathrm{Hom}_{\mathcal{C}}(X, Y)$: the compositions $X \to Z \to Y$ as above yield $|F(Y)|$ distinct morphisms, one for each projection, and by Proposition 3.9, these must be all of them.

It remains to show that X is Galois, i.e. $\mathrm{Aut}(X)$ acts transitively on $F(X)$. Let $x' \in F(X)$. The map $\mathrm{Hom}_{\mathcal{C}}(X, Y) \to F(Y)$, $\phi \mapsto F(\phi)(x')$ is bijective, since $|\mathrm{Hom}_{\mathcal{C}}(X, Y)| = |F(Y)|$ and we already know the map is injective. Since the morphisms $F(\phi)$ correspond to projecting x' onto some coordinate, this shows that $x' = (x_{\sigma(1)}, \ldots, x_{\sigma(|F(Y)|)})$ as an element of $F(Z)$, where σ is some permutation on $|F(Y)|$ letters. σ comes from an automorphism $\tilde{\sigma}$ of Z permuting the terms of the product, which must send X to another connected component X' (recall that the decomposition into connected components is unique). But $x' \in F(X) \cap F(X')$, so by connectedness $X = X'$. So $\tilde{\sigma}$ restricts to an automorphism of X which sends x to x', proving the remaining part of the claim.

Now suppose Y is connected. Let X be the Galois object from above, and fix some $x \in F(X)$. $\mathrm{Aut}(X)$ acts on $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ from the right by composition. This action is transitive: let $\phi, \psi : X \to Y$. By Lemma 3.6, $F(\psi)$ is surjective, so let $a \in F(X)$ such that $F(\phi)(x) = F(\psi)(a)$. X is Galois, so we may pick an automorphism σ such that $F(\sigma)(a) = x$. It follows that $F(\phi \circ \sigma)(a) = F(\psi)(a)$, and by Corollary 3.10 we get $\phi \circ \sigma = \psi$, as required.

Let $\phi \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ and let G be its stabilizer; i.e. $G = \{\sigma \in \mathrm{Aut}(X) \mid \phi \circ \sigma = \phi\} \leq \mathrm{Aut}(X)$. ϕ factors through a morphism $\tilde{\phi} : X/G \to Y$. We will show that this is in fact an isomorphism, which will imply the result. Since F is conservative, it is enough to show that $F(\tilde{\phi}) : F(X)/G \to F(Y)$ is a bijection. Surjectivity is immediate from surjectivity of $F(\phi)$ (Lemma 3.6). Moreover, $|F(Y)| = |\mathrm{Hom}_{\mathcal{C}}(X, Y)| = [\mathrm{Aut}(X) : G]$ by the orbit-stabilizer theorem (Theorem 1.3) together with the fact that the action is transitive. By the above remark, G acts freely on $F(X)$, which implies that $|F(X)/G| = |F(X)|/|G| = |\mathrm{Aut}(X)|/|G| = [\mathrm{Aut}(X) : G]$ too. So $F(\tilde{\phi})$ is indeed a bijection, and we are done. □

3.4 Automorphism groups of functors and the Galois correspondence

When discussing functors previously, we mentioned that functors mapping from $\mathcal{C}_1$ to $\mathcal{C}_2$ form a category in their own right. Given an object X in any category, we can look at the group $\mathrm{Aut}(X)$ of isomorphisms $X \to X$. It turns out that the automorphism group of a fundamental functor has some interesting properties.

Proposition 3.14. Let $F : \mathcal{C} \to \mathsf{FSet}$ be a functor from a small category $\mathcal{C}$ to the category of finite sets. Then $\mathrm{Aut}(F)$ is a profinite group.

Proof. By definition, any automorphism of F consists of a collection of invertible set-functions $\sigma_X : F(X) \to F(X)$, one for each $X \in \mathrm{Obj}(\mathcal{C})$, such that all diagrams

$$\begin{array}{ccc} F(X) & \xrightarrow{\sigma_X} & F(X) \\ {\scriptstyle F(\phi)}\downarrow & & \downarrow{\scriptstyle F(\phi)} \\ F(Y) & \xrightarrow{\sigma_Y} & F(Y) \end{array}$$

commute. Since each σ_X has to be a bijection, $\mathrm{Aut}(F)$ is a subgroup of

$$G = \prod_{X \in \mathrm{Obj}(\mathcal{C})} \mathfrak{S}(F(X)),$$

where $\mathfrak{S}(F(X))$ is the group of bijections $F(X) \to F(X)$, so that $|\mathfrak{S}(F(X))| = |F(X)|!$; we are taking $\mathcal{C}$ to be small so that this product makes sense. We endow each $\mathfrak{S}(F(X))$ with the discrete topology and G with the product topology, turning G into a profinite group. Since closed subgroups of profinite groups are profinite, it suffices to show that $\mathrm{Aut}(F)$ is closed in G. We have

$$\mathrm{Aut}(F) = \bigcap_{\substack{Y,Z \in \mathrm{Obj}(\mathcal{C}) \\ \phi \in \mathrm{Hom}_{\mathcal{C}}(Y,Z)}} \{G \ni (\sigma_X)_{X \in \mathrm{Obj}(\mathcal{C})} \mid F(\phi) \circ \sigma_Y = \sigma_Z \circ F(\phi)\}.$$

Now each of these subsets is closed. Indeed, fix Y, Z and ϕ, and suppose $F(\phi) \circ \sigma_Y \neq \sigma_Z \circ F(\phi)$ for some element (σ_X). Then

$$(\ldots, \mathfrak{S}(F(X_i)), \ldots, \sigma_Z, \ldots, \sigma_Y, \ldots, \mathfrak{S}(F(X_1)))$$

is an open neighbourhood of (σ_X) contained in the complement of the subset we were considering. Thus, $\mathrm{Aut}(F)$ is an intersection of closed subsets and hence is itself closed; thus it is a profinite group. □

In the above proposition, it is actually enough for $\mathcal{C}$ to be *essentially small*, i.e. equivalent to a small category. When we use the proposition in what follows, the relevant categories will always be essentially small, so we will not care much about this condition.

Example 3.15. Let G be a group, and $F : G\text{-}\mathsf{Set} \to \mathsf{Set}$ the forgetful functor. What is $\mathrm{Aut}(F)$? Well, for any element $g \in G$, we can construct an automorphism of F by sending $s \mapsto gs$ for

$s \in F(S)$ for any G-set S: this makes all squares

$$\begin{array}{ccc} F(A) & \xrightarrow{g} & F(A) \\ {\scriptstyle F(\phi)}\downarrow & & \downarrow{\scriptstyle F(\phi)} \\ F(B) & \xrightarrow{g} & F(B) \end{array}$$

commute, because $\phi : A \to B$ is a morphism of G-sets.
The above map $G \to \mathrm{Aut}(F)$ is clearly a group homomorphism. In fact, it is an isomorphism. To see this, note that G is itself a G-set, acting on itself by multiplication. Let (σ_S) be an automorphism of F, indexed by $\mathrm{Obj}(G\text{-}\mathsf{Set})$. Now $\sigma_G(e) \in G$, and the map $(\sigma_S) \mapsto \sigma_G(e)$ is inverse to our previous map. Indeed, the automorphism induced by $g \in G$ sends $e \mapsto g$. Going the other way, we need to show that $\sigma_S(s) = \sigma_G(e)(s)$ for any G-set S and $s \in S$. For any such s, we have a morphism of G-sets $f_s : G \to S$, $g \mapsto gs$. As such, it satisfies $\sigma_S \circ F(f_s) = F(f_s) \circ \sigma_G$. Evaluating this expression at $e \in G$, we get $\sigma_S(s) = \sigma_G(e)(s)$, as required. So $\mathrm{Aut}(F) \cong G$. ⧫

An important observation is that automorphism groups of functors are invariant under composition with equivalences. More precisely, if $E : \mathcal{C}_1 \to \mathcal{C}_2$ is an equivalence and if $F_1 : \mathcal{C}_1 \to \mathcal{D}$, $F_2 : \mathcal{C}_2 \to \mathcal{D}$ are functors such that $F_1 = F_2 \circ E$, then $\mathrm{Aut}(F_1) \cong \mathrm{Aut}(F_2)$. Clearly $\mathrm{Aut}(F_1) = \mathrm{Aut}(F_2 \circ E)$; the statement holds because if $\sigma_X : F_2(X) \to F_2(X)$ is an isomorphism commuting with the maps $F_2(\phi)$ for $\phi \in \mathrm{Hom}_{\mathcal{C}_2}(X, Y)$, then $F_2(E(E^{-1}(\sigma_X)))$ will also be an isomorphism commuting with the respective maps, where E^{-1} is the quasi-inverse of E. This gives an isomorphism $\mathrm{Aut}(F_2) \to \mathrm{Aut}(F_2 \circ E)$, so indeed $\mathrm{Aut}(F_1) \cong \mathrm{Aut}(F_2)$.

The automorphism group of a fundamental functor F has an action on any finite set $F(X)$: we can first project any element $(\sigma_Y)_{Y \in \mathrm{Obj}(\mathcal{C})}$ down to $\sigma_X \in \mathfrak{S}(F(X))$, which then acts on $F(X)$ by sending $x \mapsto \sigma_X(x)$.

Proposition 3.16. Let $X \in \mathrm{Obj}(\mathcal{C})$ and consider $F(X)$ as a discrete topological space. Then the action of $\mathrm{Aut}(F)$ on $F(X)$ is continuous.

Proof. By Proposition 4.8, we need to check that stabilizers are open. Since $\mathrm{Aut}(F)$ acts through the factor $\mathrm{Aut}(F(X))$, the stabilizer of an arbitrary $x \in F(X)$ is

$$\mathrm{Aut}(F) \cap \left(\mathrm{Stab}_{\mathfrak{S}(F(X))}(x) \times \prod_{Y \neq X} \mathfrak{S}(F(Y)) \right).$$

Since each $\mathfrak{S}(F(X))$ is discrete and $\mathrm{Aut}(F)$ carries the subspace topology, this is an open set. □

See Examples 4.8 for examples of continuous and discontinuous actions of a profinite group on finite sets.

Note that the morphisms $F(\phi)$ in FSet are actually morphisms of finite $\mathrm{Aut}(F)$-sets; this follows directly from the commutative square we drew in the proof of Proposition 3.14. Thus, if we denote by $\mathrm{Aut}(F)$-FSet the category of finite sets with a continuous left $\mathrm{Aut}(F)$-action, we can extend F to a functor $\bar{F} : \mathcal{C} \to \mathrm{Aut}(F)$-$\mathsf{FSet}$. Explicitly, $F = G \circ \bar{F}$, where $G : \mathrm{Aut}(F)$-$\mathsf{FSet} \to \mathsf{FSet}$ is the forgetful functor.

We are now ready to prove the main theorem of Galois categories.

Theorem 3.17 (Grothendieck)**.** Let $(\mathcal{C}, F)$ be a Galois category. $\bar{F}$ induces an equivalence between $\mathcal{C}$ and $\mathrm{Aut}(F)$-FSet, and if $\mathcal{C}$ is equivalent to π-FSet for some profinite group π in such a way that F is the composition of this equivalence with the forgetful functor to FSet, then $\pi \cong \mathrm{Aut}(F)$.

Proof. Let I be the set of pairs (X, x) where X is a connected object and $x \in F(X)$. For $(X, x), (Y, y) \in I$, we say $(X, x) \geq (Y, y)$ if there is some $\phi \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ such that $F(\phi)(x) = y$. This ϕ is unique if it exists, by Corollary 3.10. In particular, if $F(\phi)(x) = y$ and $F(\psi)(y) = x$, then $\psi \circ \phi = \mathrm{Id}_X$ and $\phi \circ \psi = \mathrm{Id}_Y$ so that X and Y are isomorphic. It follows that $\geq$ is a partial order on isomorphism classes of I. In fact, the order is directed, i.e. for any (X, x) and (Y, y), there is some (Z, z) with $(Z, z) \geq (X, x)$ and $(Z, z) \geq (Y, y)$. Indeed, we can take Z to be the connected component of $X \times Y$ for which $(x, y) \in F(Z)$. Exactness of F implies that the canonical morphisms π_X and π_Y, from the product to X and Y respectively, turn into the set-theoretic projections under F, so that $F(\pi_X)(z) = x$ and $F(\pi_Y)(z) = y$, as required.
Let $\mathcal{I}$ denote the category where $\mathrm{Obj}(\mathcal{I})$ is the set I, and

$$\mathrm{Hom}_{\mathcal{I}}((X, x), (Y, y)) = \begin{cases} \{\phi\} & \text{if } (X, x) \geq (Y, y); \\ \emptyset & \text{otherwise,} \end{cases}$$

where $\phi : (X, x) \to (Y, y)$ is the unique map $\phi : X \to Y$ such that $F(\phi)(x) = y$, if it exists.
Let Z be any object in $\mathcal{C}$. Consider again the injective maps $\mathrm{Hom}_{\mathcal{C}}(X, Z) \to F(Z)$ for $(X, x) \in \mathrm{Obj}(\mathcal{I})$. If $(X, x) \geq (Y, y)$, we obtain a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(Y, Z) & & \\ \Big\downarrow{\scriptstyle \phi^*} & \searrow & \\ & & F(Z) \\ \mathrm{Hom}_{\mathcal{C}}(X, Z) & \nearrow & \end{array}$$

where $\phi^* : \psi \mapsto \psi \circ \phi$. Let G_Z be the contravariant functor $\mathcal{I} \to \mathsf{FSet}$ sending $(X, x) \mapsto \mathrm{Hom}_{\mathcal{C}}(X, Z)$ and $\phi \mapsto \phi^*$. By the above diagram, we have an induced map $\varinjlim G_Z \to F(Z)$.

This map is a bijection. Indeed, the map is injective by injectivity of the maps $\mathrm{Hom}_{\mathcal{C}}(X, Z) \to F(Z)$. For surjectivity, we note that any $z \in F(Z)$ is contained in $F(C)$, where C is a connected component of Z. Since F sends the subobject $m : C \to Z$ to the inclusion $F(C) \hookrightarrow F(Z)$, we have $F(m)(z) = z$, where now $(C, z) \in \mathrm{Obj}(\mathcal{I})$. This proves the claim that $\varinjlim G_Z \cong F(Z)$.

We now observe that if we have a morphism $\phi \in \mathrm{Hom}_{\mathcal{C}}(Z, Z')$, we have a map $\phi_* : \mathrm{Hom}_{\mathcal{C}}(X, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z')$ for each $(X, x) \in \mathrm{Obj}(\mathcal{I})$, given by composition with ϕ on the left. This induces a morphism of injective limits, making the diagram

$$\begin{array}{ccc} \varinjlim G_Z & \longrightarrow & F(Z) \\ \Big\downarrow & & \Big\downarrow \\ \varinjlim G_{Z'} & \longrightarrow & F(Z') \end{array}$$

commute; since the horizontal maps are isomorphisms, we conclude that F is isomorphic to the functor $\varinjlim G_\bullet$. In other words, $F \cong \varinjlim \mathrm{Hom}_{\mathcal{C}}(X, \bullet)$ as X ranges over $\mathcal{I}^{\mathrm{op}}$. (This can be phrased

as saying that F is *pro-representable*.)

Denote by $\mathcal{I}_{\mathrm{Gal}}$ the subcategory of $\mathcal{I}$ consisting of all pairs (X, x) where X is Galois. If $(Y, y) \in \mathrm{Obj}(\mathcal{I})$, Y is the quotient of a Galois object X by a subgroup of $\mathrm{Aut}(X)$. In particular, there is a morphism $\phi : X \to Y$, and by connectedness of Y, $F(\phi)$ is surjective. Hence, there is $x \in F(X)$ such that $F(\phi)(x) = y$, and we get that $(X, x) \geq (Y, y)$. This shows that $\mathcal{I}_{\mathrm{Gal}}$ is *cofinal* in $\mathcal{I}$. The colimit of a functor $\mathcal{J} \to \mathcal{C}$ is the same as taking the colimit of the restriction of that functor to a cofinal subcategory of $\mathcal{J}$, so in this case we have $F \cong \varinjlim G'_\bullet$, where G'_Z is the restriction of G_Z to $\mathcal{I}_{\mathrm{Gal}}$ for each $Z \in \mathcal{C}$.

Now let $\phi : (X, x) \to (Y, y)$ in $\mathcal{I}_{\mathrm{Gal}}$. Because Y is Galois, we know that $\mathrm{Aut}(Y)$ acts freely and transitively on $F(Y)$. Thus, for any $\sigma \in \mathrm{Aut}(X)$ we can find a unique $\tau \in \mathrm{Aut}(Y)$ such that $F(\phi \circ \sigma)(x) = F(\tau)(y) = F(\tau \circ \phi)(x)$, so by Corollary 3.10 we have $\phi \circ \sigma = \tau \circ \phi$. Define a homomorphism $\phi_{XY} : \mathrm{Aut}(X) \to \mathrm{Aut}(Y)$ by sending $\sigma \mapsto \tau$ in this way; it is easily checked from the basic properties of functors that this really is a homomorphism. Moreover, ϕ_{XY} is surjective: this is the case because the right action of $\mathrm{Aut}(X)$ on $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is transitive, i.e. any $\tau \circ \phi$ can be written as $\phi \circ \sigma$ for some $\sigma \in \mathrm{Aut}(X)$. (Transitivity of the action was proved in Theorem 3.13.) Note that $\phi_{XX} = \mathrm{Id}_X$, and $\phi_{XZ} = \phi_{YZ} \circ \phi_{XY}$. Thus, $(\mathrm{Aut}(X), \phi_{XY})$ where X ranges over isomorphism classes of Galois objects of $\mathcal{C}$ is a projective system of finite groups. We define $\pi := \varprojlim \mathrm{Aut}(X)$.

We now construct a functor $\widetilde{F} : \mathcal{C} \to \pi\text{-}\mathsf{FSet}$. For each $Z \in \mathrm{Obj}(\mathcal{C})$, we have a continuous action of π on $F(Z) \cong \varinjlim G'_Z$, explained now: if X is any Galois object, $\mathrm{Aut}(X)$ acts on $\mathrm{Hom}_{\mathcal{C}}(X, Z)$ by the map $(\sigma, \phi) \mapsto \phi\sigma^{-1}$, and a routine check shows that for $(X, x) \geq (Y, y)$, the diagram

$$\begin{array}{ccc} \mathrm{Aut}(X) & \overset{\text{acts}}{\cdots\cdots\rightarrow} & \mathrm{Hom}_{\mathcal{C}}(X, Z) \\ {\scriptstyle \phi_{XY}}\downarrow & & \uparrow{\scriptstyle \phi^*} \\ \mathrm{Aut}(Y) & \overset{\text{acts}}{\cdots\cdots\rightarrow} & \mathrm{Hom}_{\mathcal{C}}(Y, Z) \end{array}$$

commutes. Thus, we have a well-defined action on $\varinjlim G'_Y$, which we may identify with $F(Z)$. We let $\widetilde{F}(Z)$ be the π-set $F(Z)$, and for $\phi \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, we let $\widetilde{F}(\phi) = F(\phi)$. For this to be a functor, we need to verify that $\widetilde{F}(\phi)$ is a morphism of π-sets; this is again routine, but quite cumbersome to show. The reader may verify on their own that this is indeed the case by considering the induced maps $\varinjlim G'_X \to \varinjlim G'_Y$ where $\phi_* : \mathrm{Hom}_{\mathcal{C}}(Z, X) \to \mathrm{Hom}_{\mathcal{C}}(Z, Y)$, for Z Galois, is given by composition with ϕ on the left.

Summarizing the above, we have constructed a functor $\widetilde{F} : \mathcal{C} \to \pi\text{-}\mathsf{FSet}$ whose composition with the forgetful functor is F. Our next goal is to prove that $\widetilde{F}$ is an equivalence. Let's show essential surjectivity. We first note that any finite π-set is the coproduct (disjoint union) of finitely many transitive π-sets (the orbits). Since both F and the forgetful functor are exact and conservative, so is $\widetilde{F}$, and therefore it is enough to show that any finite transitive π-set is isomorphic to some $\widetilde{F}(Y)$. By considering the way π acts on finite sets, we see that transitive sets are those of the form $\mathrm{Aut}(X)/G$, where X is Galois and $G \leq \mathrm{Aut}(X)$. Let $x \in F(X)$. As shown before, the map $\mathrm{Aut}(X) \to F(X)$ given by $\phi \mapsto F(\phi)(x)$ is a bijection. $\widetilde{F}(X)$ is $F(X)$ with the action of π which sends $(\sigma, F(\phi)(x)) \mapsto F(\phi \circ \sigma^{-1})(x)$, so $\widetilde{F}(X)$ is isomorphic as a π-set to $\mathrm{Aut}(X)$, where

now π acts by composition on the left, under the map $F(\phi)(x) \mapsto \phi^{-1}$. Thus, the quotient object $\widetilde{F}(X)/G$ in π-FSet is $\mathrm{Aut}(X)/G$. But $\widetilde{F}(X)/G = \widetilde{F}(X/G)$ (since this holds for F), and so $\widetilde{F}(X/G) \cong \mathrm{Aut}(X)/G$, showing $\widetilde{F}$ is essentially surjective.

Next, we want to show that $|\mathrm{Hom}_{\mathcal{C}}(X,Y)| = |\mathrm{Hom}_{\pi}(\widetilde{F}(X), \widetilde{F}(Y))|$ for any two objects X, Y of $\mathcal{C}$, where of course π is shorthand for π-FSet. We first show that $\phi \mapsto \widetilde{F}(\phi)$ is injective. Suppose $\widetilde{F}(\phi) = \widetilde{F}(\psi)$. Then the equalizer of ϕ and ψ in $\mathcal{C}$ is X, using exactness of $\widetilde{F}$. But this says exactly that $\phi = \psi$.

Decomposing X into connected components $X_1, \ldots, X_n$, we have $\mathrm{Hom}_{\mathcal{C}}(X,Y) \cong \prod_{i=1}^{n} \mathrm{Hom}_{\mathcal{C}}(X_i, Y)$, and similarly by exactness of $\widetilde{F}$ we have $\mathrm{Hom}_{\pi}(\widetilde{F}(X), \widetilde{F}(Y)) \cong \prod_{i=1}^{n} \mathrm{Hom}_{\pi}(\widetilde{F}(X_i), \widetilde{F}(Y))$. Hence, it suffices to consider the case where X is connected. Given a morphism $X \to Y$, we can factorize it as $X \to Z \to Y$, a composition of a monomorphism of an epimorphism. By Lemma 3.8, Z is connected, so it is in fact one of the connected components of Y. Write $Y = \coprod_{i=1}^{m} Y_i$. Using connectedness of X, we have $\mathrm{Hom}_{\mathcal{C}}(X,Y) \cong \coprod_{i=1}^{m} \mathrm{Hom}_{\mathcal{C}}(X, Y_i)$. Again, there is such a decomposition for $\mathrm{Hom}_{\pi}(\widetilde{F}(X), \widetilde{F}(Y))$ too, so we may assume that Y is also connected.

We now show that $|\mathrm{Hom}_{\mathcal{C}}(X,Y)| = |\mathrm{Hom}_{\pi}(\widetilde{F}(X), \widetilde{F}(Y))|$ for X and Y connected. Using Theorem 3.13, we can write $X = C/G_1$, $Y = C/G_2$ for some large enough $(C, c) \in \mathcal{I}_{\mathrm{Gal}}$ (with respect to our directed order). Thus, $\widetilde{F}(X) \cong \mathrm{Aut}(C)/G_1$ and $\widetilde{F}(Y) \cong \mathrm{Aut}(C)/G_2$ as π-sets, as shown before. Any morphism of π-sets $\widetilde{F}(X) \to \widetilde{F}(Y)$ is given by a map $[\sigma] \mapsto [\sigma\tau]$ for some $[\tau] \in \mathrm{Aut}(C)/G_2$, which is well-defined if and only if $G_1\tau \subseteq \tau G_2$. Thus, $|\mathrm{Hom}_{\pi}(\widetilde{F}(X), \widetilde{F}(Y))| = |\{\tau G_2 \in \mathrm{Aut}(C)/G_2 \mid G_1\tau \subseteq \tau G_2\}|$. Let now $\phi \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$. We have canonical quotient morphisms $p_X : C \to X$ and $p_Y : C \to Y$. $F(p_Y)$ is surjective, so let $c' \in F(C)$ be such that $F(p_Y)(c') = F(\phi \circ p_X)(c)$. Let $\sigma \in \mathrm{Aut}(C)$ be such that $F(\sigma)(c) = c'$; then $p_Y \circ \sigma = f \circ p_X$. Moreover, f uniquely determines σG_2, since

$$h_2\sigma = h_2\sigma' \iff \sigma'\sigma^{-1} \in G_2 \iff G_2\sigma = G_2\sigma'.$$

Conversely, for an automorphism $\sigma \in \mathrm{Aut}(C)$, we can find $\phi : X \to Y$ such that $\phi \circ p_X = p_Y \circ \sigma$ if and only if $p_Y \circ \sigma$ factors through $\mathrm{Aut}(C)/G_1$, i.e. $p_Y \circ \sigma \circ \sigma' = p_Y \circ \sigma$ for all $\sigma' \in G_1$, i.e. $\sigma G_1 \subseteq G_2\sigma$. We have shown that $|\mathrm{Hom}_{\mathcal{C}}(X,Y)| = |\{G_2\sigma \mid \sigma G_1 \subseteq G_2\sigma\}|$. Thus, the map $\mathrm{Hom}_{\mathcal{C}}(X,Y) = \mathrm{Hom}_{\pi}(\widetilde{F}(X), \widetilde{F}(Y))$ is a bijection, which shows essential surjectivity. Thus, $\widetilde{F}$ is an equivalence between $\mathcal{C}$ and π-FSet.

We are finally ready to prove the statement of the theorem. We first prove the second part: suppose π is any profinite group and $H : \mathcal{C} \to \pi$-FSet an equivalence such that $F = G \circ H$, G being the forgetful functor. We have $\mathrm{Aut}(F) \cong \mathrm{Aut}(G)$ since H is an equivalence, and by Example 3.15 we know that $\mathrm{Aut}(G) \cong \pi$. Thus, $\mathrm{Aut}(F) \cong \pi$, as required.

Let now π be the profinite group constructed earlier in this proof; using what we just showed, we have $\pi \cong \mathrm{Aut}(F)$, and so $\widetilde{F} : \mathcal{C} \to \pi$-$\mathsf{FSet}$ is isomorphic to a functor $\mathcal{C} \to \mathrm{Aut}(F)$-$\mathsf{FSet}$. But from our construction, this latter functor is just $\bar{F}$. Since we showed that $\widetilde{F}$ is an equivalence, $\bar{F}$ is an equivalence, and we are done. □

The proof also shows that Galois categories are well-defined:

Corollary 3.18. If F and F' are two fundamental functors for a Galois category $\mathcal{C}$, then they are isomorphic.

Proof. Recall our construction of $\mathcal{I}_{\mathrm{Gal}}$: the objects are pairs (X, x) where X is Galois and $x \in F(X)$. Denote by $\mathcal{I}'_{\mathrm{Gal}}$ the corresponding category for F'. For $Z \in \mathrm{Obj}(\mathcal{C})$, let $H_Z : \mathcal{I}_{\mathrm{Gal}} \to \mathsf{FSet}$ be the functor earlier denoted G'_Z, and let H'_Z be the corresponding functor with domain $\mathcal{I}'_{\mathrm{Gal}}$. We have $F \cong \varinjlim H_\bullet$ and $F' \cong \varinjlim H'_\bullet$. To prove the corollary, it is enough to show that $\varinjlim H_\bullet \cong \varinjlim H'_\bullet$.

We may replace $\mathcal{I}_{\mathrm{Gal}}$ and $\mathcal{I}'_{\mathrm{Gal}}$ by their respective subcategories which contain a unique object (X, x) for any Galois object X, where $x \in F(X)$ for $\mathcal{I}_{\mathrm{Gal}}$ and $x \in F'(X)$ for $\mathcal{I}'_{\mathrm{Gal}}$; we showed already that (X, x) and (X, y) were isomorphic, so we are now looking at isomorphism classes. Of course, if $(X, x) \geq (Y, y)$ in $\mathcal{I}_{\mathrm{Gal}}$, then $(X, x') \geq (Y, y')$ in $\mathcal{I}'_{\mathrm{Gal}}$, only the morphisms ϕ and ϕ' such that $F(\phi)(x) = y$, $F'(\phi')(x') = y'$ may differ. However, since automorphism groups of Galois objects act freely and transitively on their images under a fundamental functor, for any $\sigma \in \mathrm{Aut}(X)$ there is a unique $\tau \in \mathrm{Aut}(Y)$ with $\tau \circ \phi = \phi \circ \sigma$. Denote by ϕ_{XY} the map $\mathrm{Aut}(X) \to \mathrm{Aut}(Y)$ sending $\sigma \mapsto \tau$; as before, we have $\phi_{XZ} = \phi_{YZ} \circ \phi_{XY}$, and so we have an inverse limit $G := \varprojlim \mathrm{Aut}(X)$, where X ranges over the Galois objects of $\mathcal{C}$.

The inverse limit of a system of finite, non-empty sets is non-empty, and so we have $(\sigma_X) \in G$ such that any diagram

$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ {\scriptstyle \sigma_X}\downarrow & & \downarrow{\scriptstyle \sigma_Y} \\ X & \xrightarrow{\phi'} & Y \end{array}$$

commutes, whenever $\phi : (X, x) \to (Y, y)$ and $\phi' : (X, x') \to (Y, y')$ are morphisms in $\mathcal{I}_{\mathrm{Gal}}$, resp. $\mathcal{I}'_{\mathrm{Gal}}$. Thus, (σ_X) induces an isomorphism $\varinjlim H_\bullet \to \varinjlim H'_\bullet$, as required. □

One would be justified in calling Theorem 3.17 the main theorem of Galois categories, or perhaps the categorical Galois correspondence: the fundamental functor F induces a correspondence between $\mathcal{C}$ and π-FSet, where $\pi = \mathrm{Aut}(F)$ is a profinite group. This gives us a way of studying $\mathcal{C}$ by understanding the behaviour of this group action.

Of course, it would be disappointing if after all this work, we found out that no Galois categories exist: the axioms are too restrictive, no non-trivial examples occur. Luckily, as any reader will undoubtedly have realised, this is not the case. We will now proceed to show that both Galois theory of fields and the theory of covering spaces in topology can be phrased in terms of Galois categories, enabling us to view these familiar theories from a new perspective.

4 Examples of Galois categories

4.1 Galois theory of fields

How does Galois theory come into play? Let k denote a base field, and let K/k be a finite Galois extension, i.e. a normal, separable extension of finite degree over k. One important observation made in the early 19^{th} century is that we can associate a group to such extensions: the Galois group $\mathrm{Gal}(K/k)$, consisting of all field automorphisms of K. The order of $\mathrm{Gal}(K/k)$ is equal to the degree of the extension, so finite extensions give rise to finite groups.
We can think about Galois groups in a slightly different way, which is more in the spirit of Galois categories.

Definition 4.1. Let k be a field. The *separable closure* of k, denoted k_s, is the subfield of the algebraic closure $\bar{k}$ consisting of all elements which are separable over k. Equivalently, k_s is the compositum of all finite separable extensions K/k contained in $\bar{k}$.

Proposition 4.2. The field extension k_s is Galois over k.

Proof. An extension K/k is Galois if and only if for any element $a \in K \setminus k$, there exists a k-automorphism ϕ of K such that $\phi(a) \neq a$. Now if $a \in \bar{k} \setminus k$ is separable over k, consider the splitting field K of a; then K is Galois, so there exists $\phi \in \mathrm{Gal}(K/k)$ such that $\phi(a) = a'$, where $a' \neq a$ is a conjugate of a; in particular, a' is separable. ϕ extends to a k-automorphism $\bar{\phi}$ of $\bar{k}$ [8, V.2.8]. Since any k-automorphism of $\bar{k}$ must send elements to their conjugates, and conjugates of separable elements are separable, we conclude that $\bar{\phi}$ restricts to an automorphism of k_s which moves a. □

Now the alternative point of view is to identify an element of $\mathrm{Gal}(K/k)$ with an embedding of K into k_s. This set of embeddings, denoted $\mathrm{Emb}_k(K, k_s)$, is in bijection with $\mathrm{Gal}(K/k)$, but is no longer a group under composition. What we get in return is an action of the absolute Galois group $\mathrm{Gal}(k) := \mathrm{Gal}(k_s/k)$, given by composition on the left. Moreover, K does not have to be Galois over k in order to talk about the set $\mathrm{Emb}_k(K, k_s)$, but merely separable. We can identify if our extension is Galois through the group action: K/k is Galois if and only if $\mathrm{Emb}_k(K, k_s)$ is isomorphic (as a $\mathrm{Gal}(k)$-set) to a finite quotient of $\mathrm{Gal}(k)$. (This follows from the infinite version of the fundamental theorem of Galois theory – see [16, 1.5.1] for a complete proof.)

In short, we have found a functor which sends finite separable extensions of k to finite sets with a $\mathrm{Gal}(k)$-action. The following theorem strongly suggests that we are actually dealing with a Galois category.

Theorem 4.3. $\mathrm{Gal}(k)$ is a profinite group.

Proof. By definition, $\mathrm{Gal}(k)$ is the group of field automorphisms of k_s leaving k fixed. We will identify this group with an inverse limit as follows.
Let $G_i = \mathrm{Gal}(L_i/k)$, where the fields L_i range over all finite Galois extensions of k; in particular, k_s/L_i for all $i \in I$. Whenever L_i contains L_j, say $i \geq j$ and define a morphism $\phi_{ij} : G_i \to G_j$ by $\sigma \mapsto \sigma|_{L_j}$. Then clearly $\phi_{jk} \circ \phi_{ij} = \phi_{ik}$, and the ordering is directed: given any two Galois extensions of k, by the primitive element theorem they are of the form $k(\alpha)$ and $k(\beta)$ for some $\alpha, \beta \in k_s$, both of which are contained in the Galois extension $k(\alpha, \beta) \subset k_s$. Thus, $((G_i)_{i\in I}, \{\phi_{ij}\})$ forms an inverse system of groups. We claim that $\varprojlim G_i \cong \mathrm{Gal}(k)$.
Define $\phi : \mathrm{Gal}(k) \to \varprojlim G_i$ by sending $\sigma \mapsto (\sigma|_{L_i})_{i\in I}$. This is clearly a morphism of groups, and has an inverse: given an element $(\sigma_i)_{i\in I}$ of the inverse limit, define $\sigma : k_s \to k_s$ by setting

$\sigma(x) = \sigma_i(x)$ whenever $x \in L_i$. This is well-defined by the compatibility requirement on the inverse limit. Hence ϕ is an isomorphism. □

To formalise the rough idea that field extensions form a Galois category, we have to find a proper fundamental functor. In order to do this, we make a slight generalisation to our domain category.

Definition 4.4. Let k be a field. A k-algebra is said to be *finite étale* if it is a finite direct sum of finite separable field extensions of k.

This clearly generalises the notion of a finite separable extension. Examples of finite étale $\mathbb{Q}$-algebras are $\mathbb{Q}$ itself, $\mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{6})$, $\mathbb{Q}\left(\sqrt[3]{3-5\sqrt{7}}\right)^5$, etc. Note that a direct sum of at least two fields is never itself a field, since there are non-zero zero divisors.
Given a field k, we now define a category FEt_k which consists of all finite étale k-algebras, including the zero algebra. The morphisms are the usual k-algebra homomorphisms.

Lemma 4.5. Let $A = \bigoplus_{i=1}^m A_i$ and $k^0 \neq B = \bigoplus_{j=1}^n B_j$ be finite étale k-algebras, where the A_i and B_j are fields. Then as sets,

$$\mathrm{Hom}_{\mathsf{FEt}_k}(A, B) \cong \prod_{j=1}^{n} \left(\coprod_{i=1}^{m} \mathrm{Emb}_k(A_i, B_j) \right).$$

In particular, if there is some j such that none of the A_i embed into B_j, then no morphisms $A \to B$ exist.

Proof. We first consider the case where $B = K$ is a field. Then any k-algebra homomorphism $A \to K$ must factor through some projection $\pi_i : A \to A_i$. To see this, let $A = \bigoplus_{i=1}^m A_i$. Let $\phi : A \to K$ be a k-algebra homomorphism. Denote by e_i the element $(0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 is in the i^{th} position. We have $\phi(e_i e_j) = \phi(0) = 0$ whenever $i \neq j$. Thus, either $\phi(e_i) = 0$ or $\phi(e_j) = 0$. Since $B \neq k^0$, there exists i such that $\phi(e_i) \neq 0$; this implies that $\phi(e_j) = 0$ for all $j \neq i$. Thus, $\phi(a_1, \ldots, a_m) = \sum_{l=1}^m \phi(0, \ldots, 0, a_l, 0, \ldots, 0)\phi(e_l) = \phi(0, \ldots, 0, a_i, 0, \ldots, 0)$, and ϕ factors through π_i, as claimed.
Since the A_i are fields, any morphism $A_i \to K$ is injective. The above shows that for any $\phi \in \mathrm{Hom}_{\mathsf{FEt}_k}(A, K)$, we have $\phi|_{A_i} \in \mathrm{Emb}_k(A_i, K)$ for some unique i. Conversely, given an embedding $f : A_i \hookrightarrow K$, we can reconstruct ϕ by setting $\phi(a_1, \ldots, a_m) = f(a_i)$. Thus, $\mathrm{Hom}_{\mathsf{FEt}_k}(A, K) \cong \coprod_{i=1}^m \mathrm{Emb}_k(A_i, K)$.
If we now let $B = \bigoplus_{i=1}^n B_i$, then by the universal property of the product, giving a morphism $A \to B$ is the same as giving morphisms $A \to B_i$ for each i. The B_i are fields, so we are in the above situation, and the lemma follows. □

We will show that the opposite category $\mathcal{C} = \mathsf{FEt}_k^{\mathrm{op}}$ is a Galois category, where $F : \mathcal{C} \to \mathsf{FSet}$ sends $A \mapsto \mathrm{Hom}_k(A, k_s)$, the set of all k-algebra homomorphisms $A \to k_s$. In the case where A is a field, this is the same as the set $\mathrm{Emb}_k(A, k_s)$ from before.

We have to work with the opposite category here, because a morphism $\phi \in \mathrm{Hom}_{\mathsf{FEt}_k}(A, B)$ gives rise to a morphism $\phi^* : \mathrm{Hom}_k(B, k_s) \to \mathrm{Hom}_k(A, k_s)$. This has implications when we try to prove that $\mathcal{C}$ is a Galois category. For example, one of the things we need to show is that any morphism ϕ in $\mathcal{C}$ is a monomorphism of an epimorphism. In opposite categories, monomorphisms turn into epimorphisms and conversely. However, we have to keep in mind that the opposite functor $\mathcal{C} \to \mathcal{C}^{\mathrm{op}}$ is contravariant, so it reverses the order of composition. Combining these two facts, we see that requiring that any morphism in $\mathcal{C}$ is a monomorphism of an epimorphism is the same thing as requiring that any morphism in $\mathcal{C}^{\mathrm{op}}$ is a monomorphism of an epimorphism:

nothing changes here, but this is not trivial.

Considering all of the four axioms we need to verify, we only really need to take care with the last one: a subobject Y of X in $\mathcal{C}$ is an epimorphism $X \to Y$ in $\mathcal{C}^{\mathrm{op}}$, that is, a surjective k-algebra homomorphism $X \to Y$. The complement of the subobject corresponds to a surjective k-algebra homomorphism $X \to Z$ such that $X \cong Y \oplus Z$. Limits transform into colimits and conversely; we still have to check the existence of both, but this distinction is important while checking exactness. Since the opposite functor is conservative, F is conservative if and only if its composition with the opposite functor is.

Theorem 4.6. The pair $(\mathcal{C} = \mathsf{FEt}_k^{\mathrm{op}}, F)$ is a Galois category, where $F(A) = \mathrm{Hom}_k(A, k_s)$.

Before we start the proof, we will briefly discuss tensor products.

Let R be a commutative ring with unity, and let A, B be R-modules. (The commutativity assumption on R can be dropped.) We denote the group operations on A and B by $+$. The *tensor product* $A \otimes_R B$ is constructed as follows. Take the free abelian group on all elements in $A \times B$, and quotient out by the relations $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$, $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$, and $(ra, b) - (a, rb)$, for all $a, a_1, a_2 \in A$; $b, b_1, b_2 \in B$; and $r \in R$. We define the tensor product to be this quotient; thus we have a quotient map $\otimes : A \times B \to A \otimes_R B$, and we denote the image of (a, b) under this map by $a \otimes b$. $A \otimes_R B$ is itself an R-module with the action given by $r(a \otimes b) = ra \otimes b = a \otimes rb$.

We say a set-function $\phi : A \times B \to G$, where G is an abelian group, is *R-balanced* if $\phi(a_1 + a_2, b) = \phi(a_1, b) + \phi(a_2, b)$, $\phi(a, b_1 + b_2) = \phi(a, b_1) + \phi(a, b_2)$, and $\phi(ra, b) = \phi(a, rb)$. The quotient map $\otimes$ is R-balanced by construction, and universally so:

Proposition 4.7. Suppose G is an abelian group, and $\phi : A \times B \to G$ is an R-balanced map. Then there exists a unique morphism of abelian groups $\psi : A \otimes_R B \to G$ such that $\phi = \psi \circ \otimes$.

Proof. Let $\psi(a \otimes b) = \phi(a, b)$. This is a well-defined homomorphism by the assumption that ϕ is R-balanced, and unique by the requirement that $\phi = \psi \circ \otimes$. □

When k is a field and A, B are k-algebras, we can turn the k-module $A \otimes_k B$ into a k-algebra by defining multiplication as $(a \otimes b)(c \otimes d) = ac \otimes bd$.
We can now prove that $\mathsf{FEt}_k^{\mathrm{op}}$ is a Galois category.

Proof of Theorem 4.6. **(Axiom 1)** We first show FEt_k has all finite limits and colimits; in this case, the opposite category will obviously also have these. By Lemma 3.2, it suffices to check the existence of fibered products, fibered coproducts, and both terminal objects. k is the initial object since any k-algebra homomorphism $k \to A$ must map k to itself. The zero k-algebra k^0 is the final object: any morphism into it is the zero map. This is the only case in which we allow 1 to be sent to 0.

Given $\phi : A \to B$ and $\psi : A \to C$, their fibered coproduct is $B \otimes_A C$. To see this, we can turn B and C into A-modules by defining the action on B by $a * b := \phi(a)b$, and the action on C by

$a * c := \psi(a)c$. We obtain a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\psi} & C \\ {\scriptstyle\phi}\downarrow & & \downarrow \\ B & \longrightarrow & B \otimes_A C \end{array},$$

where the maps from B and C to the tensor product are given by $b \mapsto b \otimes 1$, $c \mapsto 1 \otimes c$, respectively. Now suppose we have a commutative diagram like the one above, with a k-algebra D in the place of $B \otimes_A C$. Write $f_B : B \to D$, $f_C : C \to D$ for the maps in this diagram. We define a function $B \times C \to D$ by $(b, c) \mapsto f_B(b)f_C(c)$. This is A-balanced: linearity in both arguments follows from the fact that f_B and f_C are k-algebra homomorphisms, and the images of $(a * b, c)$ and $(b, a * c)$ are equal because $f_B \circ \phi = f_C \circ \psi$. By the universal property of tensor products, this gives a unique map $B \otimes_A C \to D$.

Fibered products also exist: given $\alpha : A \to C$ and $\beta : B \to C$, the fibered product is given by $A \times_C B = \{(a, b) \in A \oplus B \mid \alpha(a) = \beta(b)\}$. Let C_i be a direct summand of C; we have seen that there exist $A_{j(i)}$ and $B_{l(i)}$ which both embed into C_i. Now the intersection $\alpha(A_{j(i)}) \cap \beta(B_{l(i)})$ is a subfield of C_i; call it D_i. By construction, $\alpha|^{-1}_{A_{j(i)}}(D_i) \cong \beta|^{-1}_{B_{l(i)}}(D_i)$; these can loosely be seen as the intersection of $A_{j(i)}$ and $B_{l(i)}$. A direct verification shows that $A \times_C B = \bigoplus_{i=1}^n D_i$, where n is the number of direct summands of C.

(Axiom 2) F is conservative and exact. For conservativity, note that by Lemma 4.5, $F(B) = \mathrm{Hom}_k(B, k_s) = \coprod_{i=1}^n \mathrm{Emb}_k(B_i, k_s)$ for any $B \in \mathrm{Obj}(\mathsf{FEt}_k)$. Let $\phi \in \mathrm{Hom}_{\mathsf{FEt}_k}(A, B)$; then each B_j has some $A_{i(j)}$ which embeds into it via ϕ. Suppose $F(\phi) = \phi^* : F(B) \to F(A)$ is a bijection. We first note that A cannot have more direct summands than B, because otherwise there would be some A_i which does not affect the image of ϕ; but then no embedding $A_i \hookrightarrow k_s$ can be mapped onto by ϕ^*. Similarly, A cannot have less direct summands than B, since then some A_k embeds into more than one of the B_j; without loss of generality say we have embeddings $A_k \hookrightarrow B_1$ and $A_k \hookrightarrow B_2$. Then composing any $f : B_1 \hookrightarrow k_s$ with a suitable automorphism yields $g : B_2 \hookrightarrow k_s$ such that $\phi^*(f) = \phi^*(g)$, which can't happen. So we obtain

$$|F(B)| = \sum_{j=1}^n |\mathrm{Emb}_k(B_j, k_s)| \geq \sum_{j=1}^n |\mathrm{Emb}_k(A_{i(j)}, k_s)| = |F(A)|,$$

and since $|F(A)| = |F(B)|$ the inequality is an equality. Since the A_i and B_i are separable, $|\mathrm{Emb}_k(A_i, k_s)| = [A_i : k]_s = [A_i : k]$, and similarly for the B_i. Since $A_{i(j)} \subseteq B_j$ for all j, we have $[B_j : k] \geq [A_{i(j)} : k]$, but by the above these are all equalities. Thus ϕ induces isomorphisms $A_{i(j)} \xrightarrow{\sim} B_j$ for all j, so $\phi : A \to B$ was indeed an isomorphism.

For exactness, it is sufficient to show that F commutes with terminal objects, fibered products, and fibered coproducts. k is initial in FEt_k, so $F(k)$ should be final in FSet. This is the case, since $\mathrm{Hom}_k(k, k_s)$ is a singleton. Similarly, $F(k^0) = \emptyset$ is initial in FSet. Next, we want to show that $F(A \otimes_C B) = F(A) \times_{F(C)} F(B) = \{(a, b) \in F(A) \times F(B) \mid f^*(a) = g^*(b)\}$, where f and g are the morphisms $C \to A$ and $C \to B$, respectively. Using the universal property of the tensor

product, we obtain the following:

$$\begin{aligned} F(A \otimes_C B) &= \mathrm{Hom}_k(A \otimes_C B, k_s) \\ &= \{C\text{-balanced maps } A \times B \to k_s\} \\ &= \{\phi \in \mathrm{Hom}_k(A \times B, k_s) \mid \phi(c * a, b) = \phi(a, c * b)\ \forall c \in C\} \\ &\cong \{(\alpha, \beta) \in \mathrm{Hom}_k(A, k_s) \times \mathrm{Hom}_k(B, k_s) \mid \alpha \circ f = \beta \circ g\}, \end{aligned}$$

where we use that any k-algebra homomorphism is already linear in both arguments, and that the map $F(A) \times F(B) \to F(A \times B)$ given by $(\alpha, \beta) \mapsto (\phi : (a, b) \mapsto \alpha(a)\beta(b))$ restricts to a bijection on the above sets. This last set is exactly the fibered product in FSet we needed.

Similarly, we want to show that $F(A \times_C B) = F(A) \sqcup_{F(C)} F(B)$, the fibered coproduct in FSet. For ease of notation, we consider the case where A, B are fields; the general case is similar. By our earlier description, $A \times_C B = D$, where D is the intersection of A and B in C.

What is the fibered coproduct in FSet? Given set-functions $f : Z \to X$, $g : Z \to Y$, we have $X \sqcup_Z Y = (X \sqcup Y)/\sim$, where $\sim$ is the relation on the disjoint union given by $x \sim y \iff f(z) = x,\ g(z) = y$ for some $z \in Z$. In our situation, F sends the morphisms of étale k-algebras $\alpha : A \hookrightarrow C$, $\beta : B \hookrightarrow C$ to the set-functions $\alpha^* : F(C) \to F(A)$ and $\beta^* : F(C) \to F(B)$, so our aim is to show that $F(D) = (F(A) \sqcup F(B))/\sim$, where $\alpha^*(\phi) \sim \beta^*(\phi)$ for $\phi : C \hookrightarrow k_s$.

Without loss of generality, assume $C = A \cdot B \subset k_s$; this does not change D or $F(A) \sqcup_{F(C)} F(B)$, since if $\phi_1, \phi_2 : C \hookrightarrow k_s$ agree on $A \cdot B$, we have $\alpha^*(\phi_1) = \alpha^*(\phi_2)$ and $\beta^*(\phi_1) = \beta^*(\phi_2)$. Since A and B are separable over k, they are separable over D, so by the primitive element theorem we may write $A = D(a)$, $B = D(b)$, and consequently $C = D(a, b)$; we may then identify α and β by the inclusions. Denote by $a = a_1, \ldots, a_n$, $b = b_1, \ldots, b_m$ the conjugates of a and b. The key point is that for any choice of i and j, there is an embedding $\phi_{ij} : C \hookrightarrow k_s$ such that $a \mapsto a_i$ and $b \mapsto b_j$, because by construction $A \cap B = D$. Moreover, α^* and β^* are surjective, so for any $\phi : A \hookrightarrow k_s$ there is some $\psi_1 : C \hookrightarrow k_s$ with $\phi = \alpha^*(\psi_1)$; and in fact, we have $\phi = \alpha^*(\psi_i)$ for $1 \le i \le m$, where $\psi_i : a \mapsto \phi(a),\ b \mapsto b_i$. In other words, ϕ is identified with m distinct elements of $F(B)$ under $\sim$. Similarly, any of those m elements is identified with n distinct elements of $F(A)$, all of which are in the same equivalence class. We conclude that $\sim$ partitions $F(A) \sqcup F(B)$ into equivalence classes of size $n + m$. Thus,

$$|F(A \times_C B)| = |F(D)| = |\mathrm{Emb}_k(D, k_s)| = [D : k]_s = [D : k],$$

and

$$|F(A) \sqcup_{F_C} F(B)| = \left|\frac{F(A) \sqcup F(B)}{\sim}\right| = \frac{[A : k] + [B : k]}{n + m} = \frac{([A : D] + [B : D])[D : k]}{[A : D] + [B : D]} = [D : k].$$

Thus, $F(A \times_C B) \cong F(A) \sqcup_{F(C)} F(B)$. In the case where A and B are k-algebras, one can use the same argument in conjunction with Lemma 4.5; this shows F is exact.

(Axiom 3) Let $\phi : A \to B$ be a morphism of k-algebras; we aim to write ϕ as a monomorphism of an epimorphism. Write $A = \bigoplus_{i=1}^m A_i$, $B = \bigoplus_{i=1}^n B_i$. ϕ is given by $\phi_1 \times \ldots \times \phi_n$, where $\phi_j = \pi_j \circ \phi$. By Lemma 4.5, each of the ϕ_j factors through some $A_{i(j)}$ (not necessarily distinct), and since $\phi_j(A_{i(j)}$ is a subfield of B_j for each j, $\phi(A)$ is a finite étale k-algebra. Thus we can decompose ϕ as

$$\bigoplus_{i=1}^m A_i \twoheadrightarrow \bigoplus_{j=1}^n \phi_j(A_{i(j)}) \hookrightarrow \bigoplus_{j=1}^n B_j,$$

the second map being the inclusion of $\phi(A)$ into B.

(Axiom 4) A subobject in $\mathcal{C}$ corresponds to a surjective morphism in FEt_k. Again using Lemma 4.5, if $\phi : \bigoplus_{i=1}^m A_i \to B$ is surjective, it means there are surjective embeddings, i.e. isomorphisms of fields, $A_{i(j)} \xrightarrow{\sim} B_j$ for each direct summand B_j of B. It follows that $B \cong \bigoplus_{i=1}^k A_i$ for some $0 \leq k \leq m$ (potentially after re-ordering the A_i), with the empty sum corresponding to the zero k-algebra. The corresponding subobject in $\mathcal{C}$ is then the projection $\bigoplus_{i=1}^m A_i \to \bigoplus_{i=k+1}^m A_i$, since this gives an isomorphism

$$\bigoplus_{i=1}^{m} A_i \longrightarrow B \oplus \bigoplus_{i=k+1}^{m} A_i.$$

□

Looking back at our treatment of abstract Galois categories, we see that the connected objects in FEt_k are the fields, and the Galois objects are the Galois extensions of k; the separable extensions correspond under F to sets with transitive $\mathrm{Aut}(F)$-action, and since $\mathrm{Aut}(F) \cong \mathrm{Gal}(k)$ (check that an automorphism of F corresponds to an automorphism of k_s and conversely), these correspond to finite index subgroups of $\mathrm{Gal}(k)$. In the case of Galois extensions, the subgroup is actually normal and we can identify the extension with a finite quotient of $\mathrm{Gal}(k)$, namely the Galois group of the extension. This way of thinking about Galois theory of fields is often referred to as "Grothendieck's Galois theory".

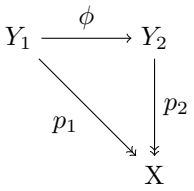
Examples 4.8.
1. Let $\mathcal{C} = \mathsf{FEt}_k^{\mathrm{op}}$ and consider the object $K := \mathbb{Q}(\omega, \sqrt[3]{2})$, i.e. the splitting field of the polynomial $X^3 - 2$. Then $F(K)$ is the set of embeddings of K into $\overline{\mathbb{Q}}$, which is in one-to-one correspondence with the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ and in particular has 6 elements. The action of $\mathrm{Aut}(F) \cong \mathrm{Gal}(\mathbb{Q})$ on this set is given by post-composition: $\phi \cdot \iota := \phi \circ \iota$ for any $\iota : K \to \overline{\mathbb{Q}}$ and $\phi \in \mathrm{Gal}(\mathbb{Q})$. The stabiliser of an embedding ι consists of those automorphisms of $\overline{\mathbb{Q}}$ which leave $\iota(K)$ fixed. Such a stabiliser is homeomorphic to $\mathrm{Gal}(K)$, which is a finite index closed subgroup of $\mathrm{Gal}(\mathbb{Q})$ and hence open. Thus, $F(K)$ is indeed a continuous $\mathrm{Aut}(F)$-set.
2. Not every action of a profinite set π on a finite set S is continuous. To see this, note that having a discontinuous action on a finite set is equivalent to having a non-open finite index subgroup of π (the kernel of the action $\pi \to \mathfrak{S}(S)$). Such subgroups exist if and only if the group is not "strongly complete". Examples of strongly complete groups are topologically finitely generated groups, such as the Galois group of a finite field or a local field. However, $\mathrm{Gal}(\mathbb{Q})$ is an example of a profinite group with non-open finite index subgroups and hence discontinuous actions on finite sets. For explicit examples, see [12, Proposition 7.26]. ♦

4.2 Covering spaces

Let X be a topological space. A *cover* or *covering space* of X is a continuous map $p : Y \to X$ such that any $x \in X$ has an open neighbourhood U such that $p^{-1}(U)$ decomposes as a disjoint union of open sets, each of which is mapped homeomorphically onto U by p. Such open sets U are called *evenly covered opens*. If X is connected, the cardinality of $p^{-1}(x)$ does not depend on x, and in this case we call $|p^{-1}(x)|$ the *degree* of the cover. We say p is a *finite* cover if the degree of p is finite.

By definition, covering spaces are surjective. Given a connected space X, we can consider the category FCov_X of finite covers of X, including the "empty cover" consisting of the empty function

$\emptyset \to X$. Morphisms are continuous maps $\phi : Y_1 \to Y_2$ compatible with the projection maps; that is, morphisms ϕ which make the diagram

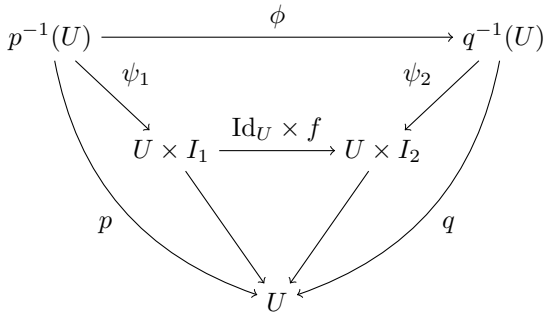


commute.
There is an obvious covariant functor $F_x : \mathsf{FCov}_X \to \mathsf{FSet}$ sending $p : Y \to X$ to the fiber $p^{-1}(x)$. If $\phi : Y_1 \to Y_2$ is a morphism of covering spaces, $F_x(\phi) : p_1^{-1}(x) \to p_2^{-1}(x)$ sends $\tilde{x} \mapsto \phi(\tilde{x})$; this is well-defined because $p_2 \circ \phi = p_1$.

Theorem 4.9. Let X be a connected topological space, and let $x \in X$. Then (FCov_X, F_x) is a Galois category.

The approach to the proof of Theorem 4.9 will be the same as the one taken for Theorem 4.6: we will check the axioms one by one. This will be less involved than in the case of fields, but we will make use of one somewhat subtle lemma:

Lemma 4.10. Let X be a topological space, $p : Y_1 \to X$ and $q : Y_2 \to X$ covering spaces, and $\phi : Y_1 \to Y_2$ a morphism of covering spaces. Then any $x \in X$ has a neighbourhood U such that the diagram



commutes, where I_1, I_2 are finite, discrete sets, ψ_1, ψ_2 are homeomorphisms, and $f : I_1 \to I_2$ is a set-function.

Proof. We first observe that any open subset of an evenly covered open is itself evenly covered. By definition, there exist opens U_p and U_q containing x such that $p^{-1}(U_p) \cong U_p \times I_1$ and $q^{-1}(U_q) \cong U_q \times I_2$; then $U' = U_p \cap U_q$ is evenly covered by both covers. The non-trivial part of the diagram requires that we show the existence of f such that it commutes with ϕ. We construct f as follows. Since ψ_1 and ψ_2 are homeomorphisms, we have a continuous map $g := \psi_2 \circ \phi \circ \psi_1^{-1} : U' \times I_1 \to U' \times I_2$. Now $g(u, i) = (u, g_u(i))$ for each $u \in U'$, where g_u is a set-function $I_1 \to I_2$, because g respects the projections to U'. We set $f := g_x$. We have a continuous map $U \times I_1 \to I_2 \times I_2$ given by $(u, i) \mapsto (f(i), g_u(i))$. By discreteness of I_2, the diagonal Δ is an open subset of $I_2 \times I_2$, so the pre-image is open; now $\{x\} \times I_1$ is contained in Δ, so it has an open neighbourhood contained in Δ, say $U \times I_1$. On U, we have $g_u = f$, and so taking U instead of U' proves the lemma. □

Proof of Theorem 4.9. **(Axiom 1)** The initial and final objects in FCov_X are the empty cover and $\mathrm{Id} : X \to X$. FCov_X has fibered products: suppose $\phi_i : Y_i \to Z$, $i = 1, 2$ are morphisms of covering spaces. Then $Y_1 \times_Z Y_2$ (which, of course, is abuse of notation: we identify covers with their domains) is $q : Y = \{(a, b) \in Y_1 \times Y_2 \mid \phi_1(a) = \phi_2(b)\} \to X$, where $q(a, b) = p(\phi_1(a)) = p(\phi_2(b))$, where $p : Z \to X$. To see that this is a finite cover of X, we use Lemma 4.10. For any $x \in X$, we can take $U_1 \ni x$ such that the lemma holds for $\phi_1 : Y_1 \to Z$, and $U_2 \ni x$ such that the lemma holds for $\phi_2 : Y_2 \to Z$; so let $U = U_1 \cap U_2$ so that the lemma holds for both these morphisms. Then U is evenly covered by q, as $q^{-1}(U) \cong U \times I$ for some finite set I.

Next, let $\psi_i : Z \to Y_i$, $i = 1, 2$. The fibered coproduct is given by $Y_1 \sqcup_Z Y_2 = (Y_1 \sqcup Y_2)/\sim_Z$, where $x \sim_Z y$ if there exists some $z \in Z$ with $\psi_1(z) = x$, $\psi_2(z) = y$. If $p_i : Y_i \to X$ are the covers, the cover from the fibered coproduct is given by

$$[v] \mapsto \begin{cases} p_1(v) & v \in Y_1; \\ p_2(v) & v \in Y_2. \end{cases}$$

This is well-defined because the ψ_i are morphisms of covering spaces, thus commute with the p_i. Again using Lemma 4.10, we see that this is indeed a covering space. By Lemma 3.2, this shows that FCov_X has all finite limits and colimits.

(Axiom 2) Exactness of F_x is immediate, since the descriptions of the fiber (co)product in FCov_X and Set are the same, and clearly $F_x(\emptyset) = \emptyset$ and $F_x(X) = \{x\}$. We show F is conservative. Let $\phi : Y \to Z$ be a morphism of covering spaces such that $F_x(\phi)$ is a bijection. Since $F_x(\phi) = \phi|_{p^{-1}(x)}$ where $p : Y \to X$ is the cover, we see that the set-function f constructed in Lemma 4.10 is a bijection. Since f is then a bijection on an open set $U \ni x$, we get that $X' := \{y \in X \mid F_y(\phi) \text{ is a bijection}\}$ is open; by the same argument, its complement is also open. $X' \neq \emptyset$ since it contains x, so by connectedness of X we get that $X = X'$; thus ϕ is a continuous bijection. Moreover, since ϕ respects the covers and evenly covered opens form a basis of X, ϕ maps open sets to open sets, so its inverse is continuous; that is, ϕ was a homeomorphism.

(Axiom 3) Let $\phi : Y \to Z$ be a morphism of covering spaces. Let $Y' \subseteq Y$ be a connected component of Y. For any $y' \in Y'$ we can find $U \ni p(y')$ such that Lemma 4.10 applies to $\phi|_{Y'}$, so $\phi(y')$ has an open neighbourhood contained in $\phi(Y')$. Similarly, if $z \in Z \setminus \phi(Y')$, z has an open neighbourhood avoiding $\phi(Y')$. This shows that the image under ϕ of each connected component of Y is open and closed in Z, thus surjective onto a connected component. Thus, we can decompose ϕ as $Y \to Z' \to Z$, where $Z' = \mathrm{Im}(\phi)$ are the connected components of Z which are mapped onto by ϕ, and $Z' \to Z$ is the inclusion.

(Axiom 4) By the above, a morphism of covering spaces $\phi : Y \to Z$ must surject any connected component of Y onto a connected component of Z. Thus, a subobject must be a bijection between some connected components of Y and Z, so we may identify Y with those connected components of Z which ϕ surjects upon. Thus, the categorical notion of connected objects corresponds to the topological notion of connectedness. The restriction of a cover to a connected component yields another cover, so if Y' is a subobject of Y, it has a complement $Y \setminus Y'$ (possibly empty). □

What does $\mathrm{Aut}(F_x)$ correspond to? We know by Theorem 3.17 that FCov_X is equivalent to the category of finite sets with a continuous action of some profinite group. Let's call this group $\pi(X) \cong \mathrm{Aut}(F_x)$. It turns out that when X is pathconnected, locally pathconnected, and semi-locally simply connected, $\pi(X)$ is the profinite completion of the fundamental group of X; one can verify this by constructing a universal cover (i.e. a simply connected cover) of X, which

exists under the given conditions (see e.g. [7, section 1.3] for details). However, X need only be connected for FCov_X to form a Galois category, so $\pi(X)$ generalizes the (profinite) fundamental group in the sense that it is equal to it when X admits a universal cover.

The connected covers in FCov_X are the covers with connected domain, and the Galois covers are those whose automorphism groups act transitively on the fibers. As in the case of separable k-algebras, this gives a Galois correspondence between connected finite coverings of X and subgroups of $\pi(X)$. Moreover, the results from Section 3 now turn into familiar statements: for instance, Corollary 3.10 says that if $p : Y \to X$ is a connected cover, and if $\phi, \psi : Y \to Z$ are morphisms of covering spaces such that $\phi(y) = \psi(y)$ for some $y \in Y$, then $\phi = \psi$.

5 Conclusion

The theory of Galois categories which we developed has allowed us to see Galois theory from a new perspective. Besides shedding light on the question *why* the Galois correspondence exists, it is most powerful because of its generality: the theories of field extensions and covering spaces both allow the development of a Galois theory, but without the language of category theory, it is difficult to pinpoint exactly where the similarity comes from.

The fact that the absolute Galois group of a field and the fundamental group of a topological space both arise as the automorphism group of a fundamental functor is not completely unexpected. This is because, once we identify field extensions with covers, we see that the field extension which does not admit any further nontrivial algebraic extensions is the algebraic closure, while the covering space which does not admit any further nontrivial covers is the universal cover. This analogy then suggests that $\mathrm{Gal}(k)$ corresponds to the automorphism group of the universal cover, i.e. it is "the fundamental group of the base field k". This leads to perhaps the most important application of the theory.

There is a Galois category which we have not discussed, namely the category of finite étale schemes over a connected scheme X. The *étale fundamental group* of X is defined to be the automorphism group of the fundamental functor for this Galois category. This is quite significant: we can study the scheme X through its étale fundamental group, a group which, unlike the Galois group or topological fundamental group, does not arise naturally.
The theory of étale fundamental groups is better documented than that of Galois categories, so the reader who is interested in this material should have no trouble finding suitable sources; [9] or [11] would seem like a good place to start.

Bibliography

[1] P. Aluffi. *Algebra: Chapter 0*. American Mathematical Society, Providence, Rhode Island, 2009.

[2] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Westview Press, Oxford, 1969.

[3] S. Awodey. *Category Theory*. Oxford University Press, New York, 2006.

[4] F. Borceux and G. Janelidze. *Galois Theories*, volume 72 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 2001.

[5] P. Freyd. *Abelian Categories*. Harper & Row, New York, Evanston & London, 1966.

[6] A. Grothendieck. *Revêtements Étales et Groupe Fondamental (SGA 1)*, volume 224 of *Lecture Notes in Mathematics*. Springer-Verlag, 1971.

[7] A. Hatcher. *Algebraic Topology*. Cambridge University Press, 2002.

[8] S. Lang. *Algebra*. Springer-Verlag, New York, 2002.

[9] H. W. Lenstra. *Galois theory for schemes*. Electronic third edition, 2008. Available from `http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf`.

[10] W. Magnus. Residually finite groups. Bulletin of the American Mathematical Society, 1969. Available from `https://pdfs.semanticscholar.org/d09b/70713fef949e2a6d9590fe0fb976a05ac09f.pdf`.

[11] J. S. Milne. Lectures on étale cohomology (v2.21), 2013. Available from `http://www.jmilne.org/math/CourseNotes/LEC.pdf`.

[12] J. S. Milne. Fields and galois theory (v4.50), 2014. Available from `https://www.jmilne.org/math/CourseNotes/FT.pdf`.

[13] J. P. Murre. *Lectures on An Introduction to Grothendieck's Theory of the Fundamental Group*. Tata Institute of Fundamental Research, Bombay, 1967. Available from `http://www.math.tifr.res.in/~publ/ln/tifr40.pdf`.

[14] B. Osserman. Inverse limits and profinite groups. Available from `https://www.math.ucdavis.edu/~osserman/classes/250C/notes/profinite.pdf`.

[15] A. N. Skorobogatov. Algebra IV, 2017. Lecture notes from a course taught at Imperial College London. Available from `http://wwwf.imperial.ac.uk/~anskor/Algebra%20IV/algebraIV.pdf`.

[16] T. Szamuely. *Galois Groups and Fundamental Groups*, volume 117 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 2009.

[17] W. Zomervrucht. Fundamental groups, 2015. Available from `http://www.math.leidenuniv.nl/~wzomervr/docs/fundamental_groups.pdf`.