Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"
Corso di Laurea Magistrale in Matematica

The étale fundamental group of a connected scheme

Supervisor:
Prof. Adrian Iovita

Student:
Paola Francesca Chilla
Student ID 1176761

Graduation Date: 27 settembre 2019

Table of contents

Introduction

The aim of this thesis is to introduce the étale fundamental group of a connected scheme, which is the analogue in algebraic geometry of the usual fundamental group of a topological space. As the fundamental group of a topological space (under some connectedness assumptions) provides a complete description of coverings of the space in terms of sets with a group action, the étale fundamental group of a connected scheme (which is a profinite group) provides a complete description of finite étale coverings of the scheme in terms of *finite* sets with a *continuous* group action. The interest of this result (which is the main one of this work) is that, while coverings are geometrical objects which might a priori be very complicated, finite sets with a continuous action of a profinite group are easy to classify: they are disjoint unions of orbits and each of these orbits is isomorphic to the quotient set of the group with respect to an open subgroup (see lemma 1.4.9).
The étale fundamental group was introduced by Alexander Grothendieck (1928-2014) in his revolutionary work [2]. Some decades later, the topic has been approached by different authors from different perspectives, depending on their preference for an abstract setting or for a more concrete one. The approach we follow is the abstract categorical one, as developed by H. W. Lenstra in [1]. Indeed, this thesis is essentially a detailed rewriting of the sections 3,4 and 5 of Lenstra's notes, with the addition of the solutions to many of the exercises.
Lenstra starts by observing the similarities between the fundamental group of a topological space (under some connectedness assumptions, namely connected, locally path-connected and semilocally simply connected) and the absolute Galois group of a field. In the first case, we have an equivalence of categories between the coverings of the space X and the sets with an action of the fundamental group $\pi(X)$. In the second case, we have an anti-equivalence of categories between finite separable K-algebras and finite sets with a continuous action of the absolute Galois group $\mathrm{Gal}(K_s/K)$ (where K_s is the separable closure of K). There are two important differences in these example: one is the fact that the latter is an anti-equivalence, while the former is an equivalence, and the other one is the finiteness assumption which is lacking in the former example, together with the fact the the usual fundamental group of a topological space is just a group, without a canonical topology on it, while the absolute Galois group of a field is a profinite group and this allows us to restrict our attention to sets with a continuous actions. The first difference is due to the fact that the category of finite separable K-algebras is actually the opposite of an important category, namely the category of finite étale coverings of $\mathrm{Spec}(K)$. Then the absolute Galois group is nothing more than an example of étale fundamental

group. The second difference, instead, is more subtle. If we require the finiteness of the coverings, the category that we obtain is equivalent to the category of finite sets with a continuous action of the profinite completion of $\pi(X)$, but we are losing the information concerning coverings that are not finite. On the other hand, a profinite fundamental group exists and allows to describe finite coverings in more general situations, requiring only that the base space is connected. While we do not deal in detail with the Galois theory of fields, which leads to the above-mentioned anti-equivalence of categories, we will discuss in depth the case of topological spaces, because it offers interesting analogies with finite étale coverings of schemes. After discussing the two aforementioned examples, Lenstra connects them to a general framework, namely that of Galois categories. Finally, he shows that finite étale coverings of a connected scheme follow the same axioms and deduces from this the existence of the étale fundamental group of a connected scheme.
Following this path, two are the major steps through which we will reach our goal. The first step is defining Galois categories and proving that each essentially small Galois category is equivalent to the category of finite sets with a continuous action of a certain profinite group, which is unique up to isomorphism (theorem 1.4.34). The second step is defining the category of finite étale coverings of a fixed scheme (with a functor to the category of finite sets) and proving that it is an essentially small Galois category (theorem 2.3.10). These steps correspond to the two chapter of this thesis: in the first one we will deal with Galois categories, following section 3 of [1], and in the second one we will study finite étale coverings,following sections 4 and 5 of [1]. Finally, in the appendix we will discuss finite coverings of topological spaces. It is worth mentioning that the definition of finite étale morphisms that we use in this thesis, namely the one introduced in [1], is not the one that is usually found in the literature. A discussion about the equivalence of the two definitions can be found in section 6 of [1] (it turns out that they are equivalent in the case of locally noetherian schemes, while in the general case our definition is stronger).

Chapter 1

Galois categories

In this chapter we will give an axiomatic treatment of Galois categories, following section 3 of [1]. A Galois category is a category with a functor to the category of finite sets such that certain axioms are satisfied. In the first section, we will describe in detail these axioms and we will analyse two basic examples: the category of finite sets (with the identity functor) and the category of finite sets with a continuous action of a profinite group (with the forgetful functor). Clearly, the first example is just a special case of the second one, obtained considering the trivial group. The main result of this chapter (theorem 1.4.34) states that any essentially small Galois category is equivalent to a category of this type. More precisely, we can attach to any essentially small Galois category $\mathbf{C}$ (with fundamental functor F) a profinite group $\pi(\mathbf{C}, F)$ (uniquely determined up to isomorphism and called the fundamental group of $\mathbf{C}$) such that $\mathbf{C}$ is equivalent to the category of finite sets with a continuous action of $\pi(\mathbf{C}, F)$. The proof of this theorem occupies the sections 2-4. It will require a deeper understanding of the functor F (see section 2) and of the "structure" of the objects of $\mathbf{C}$. The fundamental group of $\mathbf{C}$ will turn out to be (isomorphic to) the automorphism group of F. We will also prove that two fundamental functors on the same Galois category must be isomorphic.

1.1 Definitions and basic examples

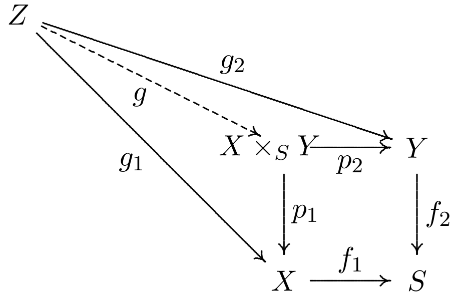
We start by recalling some definitions in category theory.

Definition 1.1.1. Let $\mathbf{C}$ be a category.

(1) An object Z of $\mathbf{C}$ is called a *terminal object* if for every object X there exists a unique morphism $X \to Z$ in $\mathbf{C}$. We denote a terminal object by 1.

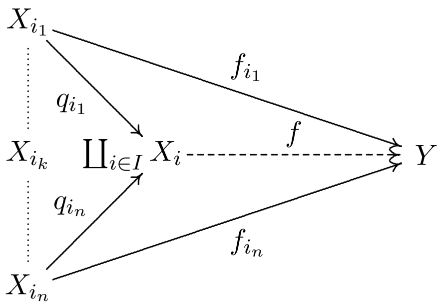
(2) Let X, Y, S be objects of $\mathbf{C}$, with two morphisms $f_1 : X \to S$, $f_2 : Y \to S$. A *fibred product* of X and Y over S is an object $X \times_S Y$, together with two morphisms $p_1 : X \times_S Y \to X$, $p_2 : X \times_S Y \to Y$, such that $f_1 \circ p_1 = f_2 \circ p_2$ and, for any object Z with morphisms $g_1 : Z \to X$, $g_2 : Z \to Y$ satisfying $f_1 \circ g_1 = f_2 \circ g_2$, there exists a unique morphism $g : Z \to X \times_S Y$ such that $g_1 = p_1 \circ g$ and $g_2 = p_2 \circ g$. This definition is illustrated by the following

commutative diagram.



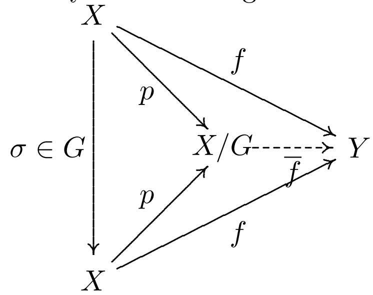
If $\mathbf{C}$ has a terminal object 1 and X, Y are objects of $\mathbf{C}$, the *product* of X and Y is defined as the fibred product $X \times_1 Y$ (with respect to the unique morphisms $X \to 1$, $Y \to 1$), if it exists, and denoted by $X \times Y$.

(3) Let $(X_i)_{i \in I}$ be a collection of objects of $\mathbf{C}$. A *sum* of the X_i's is an object $\coprod_{i \in I} X_i$, together with morphisms $q_j : X_j \to \coprod_{i \in I} X_i$ for any $j \in I$, such that, for any object Y and any collection of morphisms $f_j : X_j \to Y$ with $j \in I$, there exists a unique morphism $f : \coprod_{i \in I} X_i \to Y$ such that $f \circ q_j = f_j$ for any $j \in I$. If I is finite and $I = \{i_1, \ldots, i_n\}$, then we can write $X_{i_1} \amalg \cdots \amalg X_{i_n}$ instead of $\coprod_{i \in I} X_i$. The definition of finite sum is illustrated by the following commutative diagram.



(4) An object X of $\mathbf{C}$ is called an *initial object* if for every object Y there exists a unique morphism $X \to Y$ in $\mathbf{C}$ (this notion is the dual of that of terminal object). We denote an initial object by 0.

(5) If X is an object of $\mathbf{C}$ and G is a finite subgroup of $\mathrm{Aut}_{\mathbf{C}}(X)$ (the group of automorphisms of X in $\mathbf{C}$), a *quotient of X by G* is an object X/G of $\mathbf{C}$, together with a morphism $p : X \to X/G$, such that $p = p \circ \sigma$ for any $\sigma \in G$ and, for any object Y with a morphism $f : X \to Y$ satisfying $f = f \circ \sigma$ for any $\sigma \in G$, there exists a unique morphism $\overline{f} : X/G \to Y$ such that $f = \overline{f} \circ p$. This definition is illustrated by the following commutative diagram.



(6) A morphism $f : X \to Y$ in $\mathbf{C}$ is called a *monomorphism* if, for every object Z and every pair of morphisms $g, h : Z \to X$, $f \circ g = f \circ h$ implies $g = h$. Instead, $f : X \to Y$ is called an *epimorphism* if, for every object Z and every pair of morphisms $g, h : Y \to Z$, $g \circ f = h \circ f$ implies $g = h$ (the notions of monomorphism and epimorphism are dual to each other).

(7) $\mathbf{C}$ is called *essentially small* if it is equivalent to a small category, i.e. one whose objects form a set.

Remark 1.1.2. (1) If an object is defined through a universal property, then it is unique up to a unique isomorphism. So each of the objects defined in 1.1.1(1)-(5), if it exists, is unique up to a unique isomorphism.

(2) From the definitions, it follows that an initial object is the sum of the empty collection of objects (i.e. the collection with $I = \emptyset$), if it exists.

Example 1.1.3. We denote by **sets** the category of *finite* sets (with morphisms given by functions between sets).

(1) A singleton $\{x\}$ is a terminal object in the category **sets**. Indeed, if X is a (finite) set there is a unique function $f : X \to \{x\}$, namely the one defined by $f(a) = x$ for any $a \in X$.

(2) If X, Y, S are finite sets, with two functions $f_1 : X \to S$, $f_2 : Y \to S$, then the fibred product of X and Y over S is

$$X \times_S Y = \{(x, y) \in X \times Y \mid f_1(x) = f_2(y)\}$$

(notice that this is also a finite set, because it is contained in the product of the finite sets X and Y), together with the projections $p_1 : X \times_S Y \to X$, $(x, y) \mapsto x$ and $p_2 : X \times_S Y \to Y$, $(x, y) \mapsto y$. Indeed, $f_1 \circ p_1 = f_2 \circ p_2$ by definition and, if Z is a (finite) set with two functions $g_1 : Z \to X$, $g_2 : Z \to Y$ such that $f_1 \circ g_1 = f_2 \circ g_2$, the function $g : Z \to X \times_S Y$, $z \mapsto (g_1(z), g_2(z))$ (notice that $(g_1(z), g_2(z))$ is really an element of $X \times_S Y$, because $f_1(g_1(z)) = f_2(g_2(z))$) is the unique function making the diagram commute.
It follows that the product of two finite sets X and Y, as defined in 1.1.1(2), coincides with their cartesian product.

(3) Let $(X_i)_{i \in I}$ be a finite collection of finite sets (i.e. I is finite). Then the disjoint union $\coprod_{i \in I} X_i$ is also a finite set. This disjoint union, together with the inclusions $q_j : X_j \to \coprod_{i \in I} X_i$ for $j \in I$, is the sum of the X_i's. Indeed, if Y is a (finite) set, with a collection of functions $f_j : X_j \to Y$ with $j \in I$, there is a unique function $f : \coprod_{i \in I} X_i \to Y$ such that $f \circ q_j = f_j$ for any $j \in I$, namely the one defined by $f(x) = f_j(x)$ if j is the unique element of I such that $x \in X_j$. Notice that it was important to assume I finite. Arbitrary sums do not exist in the category of finite sets.

(4) From the previous point and from remark 1.1.2(2), it is clear that the empty set is an initial object in **sets**.

(5) Let X be a finite set and G a finite subgroup of $\mathrm{Aut}_{\mathbf{sets}}(X) = \mathrm{S}_X$ (the symmetric group on X). Then the quotient of X by G is the set of orbits of X under G: $X/G = \{Gx \mid x \in X\}$ (this is also a finite set, because it is smaller than X), together with the map $p : X \to X/G,\ x \mapsto Gx$. Indeed, if $\sigma \in G$ we have $f(\sigma x) = G\sigma x = Gx = f(x)$ for any $x \in X$ and, if Y is a (finite) set with a function $f : X \to Y$ satisfying $f = f \circ \sigma$ for any $\sigma \in G$, then the function $\overline{f} : X/G \to Y,\ Gx \mapsto f(x)$ is well defined and is the unique function making the diagram commute.

(6) If $f : X \to Y$ is a function between finite sets, then f is a monomorphism if and only if it is injective. Indeed, assume that f is injective and let $g, h : Z \to X$ be two functions such that $f \circ g = f \circ h$ (with Z a finite set). Then, for any $z \in Z$, we have $f(g(z)) = h(g(z))$, which implies $g(z) = h(z)$ by the injectivity of f. So $g = h$. Conversely, assume that f is a monomorphism and $x_1, x_2 \in X$ are such that $f(x_1) = f(x_2)$. Take Z to be the singleton $\{a\}$ and define the functions $g : Z \to X,\ a \mapsto x_1$ and $h : Z \to X,\ a \mapsto x_2$. Then $f(g(a)) = f(x_1) = f(x_2) = f(h(a))$, which means that $f \circ g = f \circ h$. Since f is a monomorphism, this implies that $g = h$. Hence $x_1 = g(a) = h(a) = x_2$. So f is injective.
On the other hand, f is an epimorphism if and only if it is surjective. Indeed, assume that f is surjective and let $g, h : Y \to Z$ be two functions such that $g \circ f = h \circ f$ (with Z a finite set). Let $y \in Y$. Since f is surjective, there exists $x \in X$ such that $y = f(x)$. Then $g(y) = g(f(x)) = h(f(x)) = h(y)$. So $g = h$. Conversely, assume that f is an epimorphism. Take Z to be the finite set $\{a, b\}$, with $a \neq b$, and define the functions $g : Y \to Z,\ y \mapsto a$ and $h : Y \to Z,\ y \mapsto \begin{cases} a & \text{if } y \in f(X) \\ b & \text{if } y \notin f(X) \end{cases}$. For any $x \in X$, we have that $f(x) \in f(X)$ and so $h(f(x)) = a = g(f(x))$. So $h \circ f = g \circ f$ and, since f is an epimorphism, $g = h$. Then for any $y \in Y$ we have $h(y) = g(y) = a$, which by definition of h implies $y \in f(X)$. Hence $Y = f(X)$, which means that f is surjective.

(7) The category **sets** is essentially small. Indeed, for any $n \in \mathbb{N}$, the sets of cardinality n are all isomorphic to each other. Then the isomorphism classes of elements of **sets** are in bijection with $\mathbb{N}$, which is a set.

We can now formulate the axioms that characterize the categories we are interested in.

Definition 1.1.4. Let $\mathbf{C}$ be a category and $F : C \to \mathbf{sets}$ a covariant functor. We say that $\mathbf{C}$ is a *Galois category* with *fundamental functor* F if the following conditions are satisfied:

(G1) there is a terminal object in $\mathbf{C}$ and the fibred product of any two objects over a third one exists in $\mathbf{C}$;

(G2) any finite collection of objects of $\mathbf{C}$ has a sum in $\mathbf{C}$ (in particular, by remark 1.1.2(2), there is an initial object in $\mathbf{C}$) and for any object X in $\mathbf{C}$ the quotient of X by any finite subgroup of $\mathrm{Aut}_{\mathbf{C}}(X)$ exists;

(G3) any morphism u in $\mathbf{C}$ can be written as $u = u' \circ u''$, where u' is a monomorphism and u'' is an epimorphism, and any monomorphism $u : X \to Y$ in $\mathbf{C}$ is an isomorphism of X with a direct summand of Y, i.e. there exist an object Z and a morphism $q_2 : Z \to Y$ such that Y, together with the morphisms $q_1 = u : X \to Y$ and $q_2 : Z \to Y$, is the sum of X and Z;

(G4) F transforms terminal objects in terminal objects and commutes with fibred products;

(G5) F commutes with finite sums, transforms epimorphisms in epimorphisms and commutes with passage to the quotient by a finite group of automorphisms (notice that, if G is a finite subgroup of $\mathrm{Aut}_{\mathbf{C}}(X)$, then $F(G)$ is a finite subgroup of $\mathrm{Aut}_{\mathbf{sets}}(F(X))$);

(G6) if u is a morphism in $\mathbf{C}$ such that $F(u)$ is an isomorphism, then u is also an isomorphism.

Example 1.1.5. By example 1.1.3(1)-(5), it follows that the category **sets** satisfies (G1) and (G2). Moreover, let X, Y be finite sets and $u : X \to Y$ a function. Then $u(X)$ is also a finite set and we can write $u = u' \circ u''$, with $u'' = u : X \to u(X)$ and $u' : u(X) \to Y$ the natural inclusion. We have that u'' is surjective, and hence an epimorphism, while u' is injective, and hence a monomorphism (see example 1.1.3(6)). This shows the first part of (G3). For the second part, if $u : X \to Y$ is a monomorphism (i.e. an injective function), we can take $Z := Y \backslash u(X)$ (this is a finite set because it is contained in Y) and $q_2 : Y \backslash u(X) \to Y$ the natural inclusion. Then $Y = u(X) \amalg (Y \backslash u(X))$, together with the natural inclusions, is a sum of $u(X)$ and $Y \backslash u(X)$ (see example 1.1.3(3)). Since u is injective, $u : X \to u(X)$ is bijective, i.e. an isomorphism of sets. Then Y, together with $q_1 = u$ and q_2, is a sum of X and Z. If we take F to be the identity functor on **sets**, then (G4), (G5), (G6) are automatically satisfied. So **sets** is a Galois category.

To introduce another example of Galois category, which will turn out to include all the other ones, we need to recall the definition of profinite group.

Definition 1.1.6. A partially ordered set I is called *directed* if for every $i, j \in I$ there exists $k \in I$ such that $k \geq i$ and $k \geq j$. A *projective system* of sets (respectively, groups or topological spaces) consists of a directed partially ordered set I, a collection of sets (respectively, groups or topological spaces) $(S_i)_{i \in I}$ and a collection of maps (respectively, group homomorphisms or continuous maps) $(f_{ij} : S_i \to S_j)_{i,j \in I,\, i \geq j}$ such that

$$\forall i \in I \qquad f_{ii} = \mathrm{id}_{S_i}$$

and

$$\forall i, j, k \in I \text{ with } i \geq j \geq k \qquad f_{ik} = f_{jk} \circ f_{ij} \,.$$

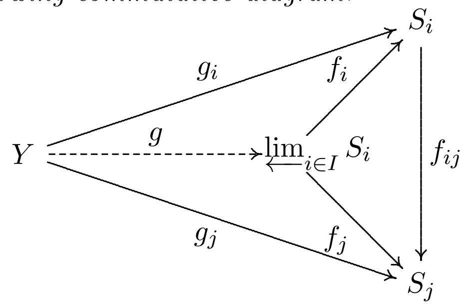
Given such a system, its *projective limit* is defined as

$$\varprojlim_{i \in I} S_i := \left\{ (x_i)_{i \in I} \in \prod_{i \in I} S_i \;\middle|\; f_{ij}(x_i) = x_j \quad \forall i, j \in I \text{ with } i \geq j \right\} \,.$$

Remark 1.1.7. (1) The projective limit of a projective system of groups is a subgroup of the direct product. In particular, it is a group. Analogously, the projective limit of a projective system of topological spaces can be seen as a topological space with the subspace topology of the product. Combining the two things, we get that the projective limit of a projective system of topological groups is a topological group.

(2) The definition of projective system can be generalized to any category. However, the projective limit in an abstract category cannot be defined as in 1.1.6.

Lemma 1.1.8 (Universal property of the projective limit)**.** *Given a projective system of sets (respectively, groups or topological spaces) as in the definition 1.1.6, let* Y *be a set (respectively, a group or a topological space) with a collection of maps (respectively, group homomorphisms or continuous maps)* $(g_j : Y \to S_j)_{j\in I}$ *such that* $g_j = f_{ij} \circ g_i$ *for any* $i, j \in I$ *with* $i \geq j$*. Then there exists a unique map (respectively, group homomorphism or continuous map)* $g : Y \to \varprojlim_{i\in I} S_i$ *such that* $g_j = f_j \circ g$ *for any* $j \in I$*, where* $f_j : \varprojlim_{i\in I} S_i \to S_j$ *is the canonical projection on the* j*-th factor. This is illustrated by the following commutative diagram.*



Proof. (Existence) Let $y \in Y$ and set $g(y) = (g_i(y))_{i\in I}$. We have to prove that $g(y) \in \varprojlim_{i\in I} S_i$. Let $i, j \in I$ such that $i \geq j$. By assumption, we have that $g_j = f_{ij} \circ g_i$. Then $f_{ij}(g_j(y)) = g_i(y)$. This shows that $g(y) \in \varprojlim_{i\in I} S_i$. So g is a well-defined map from Y to $\varprojlim_{i\in I} S_i$. Let $j \in I$. For any $y \in Y$, we have that $(f_j \circ g)(y) = f_j(g(y)) = g_j(y)$. Then $f_j \circ g = g_j$, as we wanted. In the case of groups, g is a group homomorphism because its components are group homomorphisms. Analogously, in the case of topological spaces g is continuous.

(Uniqueness) Consider a map $\widetilde{g} : Y \to \varprojlim_{i\in I} S_i$ such that $g_j = f_j \circ \widetilde{g}$ for any $j \in I$. Let $y \in Y$. For any $j \in I$, we have that $f_j(\widetilde{g}(y)) = g_j(y)$. Then $\widetilde{g}(y) = (f_i(\widetilde{g}(y)))_{i\in I} = (g_i(y))_{i\in I} = g(y)$. Hence $\widetilde{g} = g$.

□

Definition 1.1.9. A *profinite group* is a topological group that is isomorphic to the projective limit of a projective system of finite groups (each endowed with the discrete topology).

Remark 1.1.10. Let $I, (\pi_i)_{i\in I}, (f_{ij} : \pi_i \to \pi_j)_{i,j\in I,\, i\geq j}$ be a projective system of finite groups, each endowed with the discrete topology. Then each π_i is compact. By Tikhonov's theorem, the product $\prod_{i\in I} \pi_i$ is also compact. By definition, $\varprojlim_{i\in I} \pi_i$ is a subspace of $\prod_{i\in I}\pi_i$. Let us prove that it is a closed subspace. We have that

$$\varprojlim_{i\in I}\pi_i=\bigcap_{\substack{k,j\in I\\ k\geq j}}\left\{x=(x_i)_{i\in I}\in\prod_{i\in I}\pi_i\;\middle|\; f_{kj}(p_k(x))=f_{kj}(x_k)=x_j=p_j(x)\right\},$$

where $p_j:\prod_{i\in I}\pi_i\to\pi_j$ is the canonical projection, for any $j\in I$. By definition of product topology, p_j is continuous for any $j\in I$. Since f_{kj} is continuous by assumption, the composition $f_{kj}\circ p_k$ is continuous for any $k,j\in I$ with $k\geq j$. Then the map $\varphi_{kj}:\prod_{i\in I}\pi_i\to\pi_j\times\pi_j,\ x\mapsto(p_j(x),f_{kj}(p_k(x)))$ is continuous (if we put the product topology on $\pi_j\times\pi_j$, which coincides with the discrete topology). For any $j\in I$, consider the diagonal $\Delta_j:=\{(\sigma,\sigma)\mid\sigma\in\pi_j\}\subseteq\pi_j\times\pi_j$. It is closed, because $\pi_j\times\pi_j$ has the discrete topology. Then

$$\varprojlim_{i\in I}\pi_i=\bigcap_{\substack{k,j\in I\\ k\geq j}}\varphi_{kj}^{-1}(\Delta_j)$$

is closed in $\prod_{i\in I}\pi_i$, because it is an intersection of closed subsets. Since $\prod_{i\in I}\pi_i$ is compact, this implies that $\varprojlim_{i\in I}\pi_i$ is compact.
Moreover, since each π_i has the discrete topology, $\prod_{i\in I}\pi_i$ is totally disconnected and Hausdorff. Then its subspace $\varprojlim_{i\in I}\pi_i$ is also totally disconnected and Hausdorff. Hence any profinite group is compact, totally disconnected and Hausdorff.

Lemma 1.1.11. *Let π be a profinite group and π' a subgroup of π. Then π' is open if and only if it is closed and of finite index.*

Proof. Assume that π' is open. Then, since π is a topological group, $\sigma\pi'$ is also open, for any $\sigma\in\pi$. Since π' is a subgroup, we have that $\pi\backslash\pi'=\bigcup_{\sigma\in\pi\backslash\pi'}\sigma\pi'$. So $\pi\backslash\pi'$ is open, which means that π' is closed. We have that $\pi=\bigcup_{\sigma\in\pi}\sigma\pi'$. Since each $\sigma\pi'$ is open and π is compact (see remark 1.1.10), the set $\{\sigma\pi'\mid\sigma\in\pi\}$ must be finite. This means that π' has finite index in π.
Conversely, assume that π' is closed and of finite index. Then, since π is a topological group, $\sigma\pi'$ is also closed, for any $\sigma\in\pi$. We have that $\pi\backslash\pi'=\bigcup_{\sigma\in\pi\backslash\pi'}\sigma\pi'$ and this is a finite union, because π' has finite index. So $\pi\backslash\pi'$ is closed, which means that π' is open. □

Definition 1.1.12. Let π be a profinite group and E a set equipped with an action of π on it. We say that the action of π on E is *continuous* if the map $\pi\times E\to E$ defining the action is continuous (where E is endowed with the discrete topology and $\pi\times E$ with the product topology). In this case, we say that E is a *π-set*. If E_1,E_2 are two π-sets, a map $f:E_1\to E_2$ is called a *morphism of π-sets* if $f(\sigma e)=\sigma f(e)$ for every $\sigma\in\pi$, $e\in E$.

Remark 1.1.13. Let π be a profinite group. For any π-set E, the identity map id_E is clearly a morphism of π-sets. Moreover, it is immediate to check that the composition of two morphisms of π-sets is again a morphism of π-sets. This shows that π-sets form a category. We will restrict our attention to *finite* π-sets. We denote the category of finite π-sets by **π-sets**.

Lemma 1.1.14. *Let π be a profinite group and E a set equipped with an action of π on it. The action is continuous if and only if, for every $e \in E$, the stabilizer $\mathrm{Stab}_\pi(e) := \{\sigma \in \pi \mid \sigma e = e\}$ is open in π. If E is finite, this is true if and only if the kernel $\pi' := \{\sigma \in \pi \mid \sigma e = e \ \forall e \in E\}$ is open in π.*

Proof. Assume the action of π on E is continuous, i.e. the map $\varphi : \pi \times E \to E$, $(\sigma, e) \mapsto \sigma e$ is continuous. Let $e \in E$. The map $f_e : \pi \to \pi \times E$, $\sigma \mapsto (\sigma, e)$ is continuous, because its components are continuous. So the composition $\varphi \circ f_e$ is continuous. We have that

$$\mathrm{Stab}_\pi(e) = \{\sigma \in \pi \mid e = \varphi(\sigma, e) = \varphi(f_e(\sigma))\} = (\varphi \circ f_e)^{-1}(\{e\}) \ .$$

Since $\{e\}$ is open in E, this implies that $\mathrm{Stab}_\pi(e)$ is open in π.
Conversely, assume that all the stabilizers are open in π. Since E has the discrete topology, to show that φ is continuous we have to prove that $\varphi^{-1}(\{e\})$ is open in π for any $e \in E$. Let $e \in E$. We have that

$$\varphi^{-1}(\{e\}) = \{(\sigma, e') \in \pi \times E \mid \sigma e' = e\} = \bigcup_{e' \in E} \left(\{\sigma \in \pi \mid \sigma e' = e\} \times \{e'\}\right) \ .$$

Since $\{e'\}$ is open in E for any $e' \in E$, if we show that $U_{e',e} := \{\sigma \in \pi \mid \sigma e' = e\}$ is open in π, then $\varphi^{-1}(\{e\})$ is open in $\pi \times E$. If $U_{e',e} = \emptyset$, then it is clearly open. Assume $U_{e',e} \neq \emptyset$. Then there exists $\sigma_0 \in U_{e',e}$. This means that $\sigma_0 e' = e$ and so $\sigma_0^{-1} e = e'$. We claim that $U_{e',e} = \mathrm{Stab}_\pi(e)\sigma_0$. If $\sigma \in U_{e',e}$, then $(\sigma\sigma_0^{-1})e = \sigma(\sigma_0^{-1}e) = \sigma e' = e$. So $\sigma\sigma_0^{-1} \in \mathrm{Stab}_\pi(e)$ and $\sigma \in \mathrm{Stab}_\pi(e)\sigma_0$. Conversely, if $\sigma \in \mathrm{Stab}_\pi(e)\sigma_0$, then there exists $\tau \in \mathrm{Stab}_\pi(e)$ such that $\sigma = \tau\sigma_0$. Then $\sigma e' = (\tau\sigma_0)e' = \tau(\sigma_0 e') = \tau e = e$. So $\sigma \in U_{e',e}$. This shows that $U_{e',e} = \mathrm{Stab}_\pi(e)\sigma_0$. Since π is a topological group, right multiplication by σ_0 is a homeomorphism. By assumption, $\mathrm{Stab}_\pi(e)$ is open. Hence $U_{e',e}$ is open, as we wanted.
Assume now that E is finite. We have that $\pi' = \bigcap_{e \in E} \mathrm{Stab}_\pi(e)$. This is a finite intersection and so, if all the stabilizers are open, the kernel is also open. Conversely, assume that the kernel is open. Let $e \in E$. Since $\pi' \subseteq \mathrm{Stab}_\pi(e)$, we have that $\mathrm{Stab}_\pi(e) = \bigcup_{\sigma \in \mathrm{Stab}_\pi(e)} \pi'\sigma$. Since π' is open, $\pi'\sigma$ is also open for any $\sigma \in \mathrm{Stab}_\pi(e)$ (because π is a topological group). Then $\mathrm{Stab}_\pi(e)$ is open. □

Proposition 1.1.15. *If π is a profinite group, the category π-**sets** with the forgetful functor $F : \pi$-**sets** $\to$ **sets** (i.e. the functor that forgets the action of π) is an essentially small Galois category.*

Proof. First of all, we prove that π-**sets** is essentially small. It is enough to show that, for any $n \in \mathbb{N}$, the collection of isomorphism classes of π-sets of cardinality n is a set. If E is a π-set of cardinality n, we can identify it with $\{1, \dots, n\}$, with the corresponding action of π. The collection of actions of π on $\{1, \dots, n\}$ is a set, because it is contained in the set of all functions from π to S_n (the symmetric group of degree n). Hence π-**sets** is essentially small.
We check now that the conditions listed in 1.1.4 are satisfied.

(G1) Consider a singleton $\{x\}$ and define on it the trivial action of π: $\sigma x = x$ for any $\sigma \in \pi$. This action is clearly continuous, because the associated map

$\pi \times \{x\} \to \{x\}$ is constant. We claim that $\{x\}$ with this action is a terminal object in **π-sets**. If X is a (finite) π-set, we have a unique map $f : X \to \{x\}$, i.e. the constant map. We only have to check that this map is a morphism of π-sets. For any $\sigma \in \pi$, $a \in X$, we have $f(\sigma a) = x = \sigma x = \sigma f(a)$.
If X, Y, S are finite π-sets, with two morphisms of π-sets $f_1 : X \to S$, $f_2 : Y \to S$, we define an action of π on the fibred product of X and Y over S as sets (as in example 1.1.3(2)) as follows: $\sigma(x, y) = (\sigma x, \sigma y)$ for any $\sigma \in \pi$, $(x, y) \in X \times_S Y$. This is well defined because $(\sigma x, \sigma y) \in X \times_S Y$. Indeed, applying the fact that f_1 and f_2 are morphisms of π-sets, we get $f_1(\sigma x) = \sigma f_1(x) = \sigma f_2(y) = f_2(\sigma y)$. This is indeed a group action because $1(x, y) = (1x, 1y) = (x, y)$ and $(\sigma\tau)(x, y) = ((\sigma\tau)x, (\sigma\tau)y) = (\sigma(\tau x), \sigma(\tau y)) = \sigma(\tau x, \tau y) = \sigma(\tau(x, y))$ for any $(x, y) \in X \times_S Y$, $\sigma, \tau \in \pi$. Moreover, the action is continuous by lemma 1.1.14, because for any $(x, y) \in X \times_S Y$ we have

$$\begin{aligned}\mathrm{Stab}_\pi((x, y)) &= \{\sigma \in \pi \mid (x, y) = \sigma(x, y) = (\sigma x, \sigma y)\} = \\ &= \{\sigma \in \pi \mid \sigma x = x,\ \sigma y = y\} = \mathrm{Stab}_\pi(x) \cap \mathrm{Stab}_\pi(y)\ ,\end{aligned}$$

so $\mathrm{Stab}_\pi((x, y))$ is open in π because it is the intersection of two open subsets.
Let us check that $X \times_S Y$, with this action and the projections $p_1 : X \times_S Y \to X$ and $p_2 : X \times_S Y \to Y$ defined as in example 1.1.3(2), is the fibred product of X and Y over S in **π-sets**. First of all, the projections are morphism of π-sets by definition of the action on $X \times_S Y$. Moreover, $f_1 \circ p_1 = f_2 \circ p_2$ and, if Z is a finite π-set with two morphisms of π-sets $g_1 : Z \to X$, $g_2 : Z \to Y$ such that $f_1 \circ g_1 = f_2 \circ g_2$, we have a unique map $g : Z \to X \times_S Y$ such that $p_1 \circ g = g_1$ and $p_2 \circ g = g_2$ as in example 1.1.3(2). We have to check that this map is a morphism of π-sets. Let $\sigma \in \pi$, $(x, y) \in X \times_S Y$. Then

$$\begin{aligned}g(\sigma(x, y)) &= g((\sigma x, \sigma y)) = (g_1(\sigma x), g_2(\sigma y)) = \\ &= (\sigma g_1(x), \sigma g_2(y)) = \sigma(g_1(x), g_2(y)) = \sigma g((x, y))\ .\end{aligned}$$

Hence g is a morphism of π-sets.

(G2) Let $(X_i)_{i \in I}$ be a finite collection of finite π-sets. We define an action of π on the disjoint union $\coprod_{i \in I} X_i$ as follows: for any $\sigma \in \pi$, $x \in \coprod_{i \in I} X_i$, $\sigma x = \sigma *_j x$, where j is the unique element of I such that $x \in X_j$ and $*_j$ denotes the action of π on X_j. This is clearly a group action and the stabilizer of $x \in \coprod_{i \in I} X_i$ in π coincides with the stabilizer of x with respect to the action of π on X_j, where j is the unique element of I such that $x \in X_j$. So the action is continuous by lemma 1.1.14, because the action on X_j is continuous for any $j \in I$. We check now that $\coprod_{i \in I} X_i$, with this action of π and the inclusions $q_j : X_j \to \coprod_{i \in I} X_i$ for $j \in I$, is the sum of the X_i's in **π-sets**. First of all, the inclusions are morphisms of π-sets by definition of the action on $\coprod_{i \in I} X_i$. Moreover, if Y is a finite π-set with morphisms of π-sets $f_j : X_j \to Y$ for $j \in I$, we have a unique map $f : \coprod_{i \in I} X_i \to Y$ such that $f \circ q_j = f_j$ for any $j \in I$, as in example 1.1.3(3). We have to check that f is a morphism of π-sets. For any $\sigma \in \pi$, $x \in \coprod_{i \in I} X_i$, we have

$$f(\sigma x) = f(\sigma *_j x) = f_j(\sigma *_j x) = \sigma f_j(x) = \sigma f(x)\ ,$$

where j is the unique element of I such that $x \in X_j$ (and then $\sigma x = \sigma *_j x \in X_j$). So f is a morphism of π-sets.
Let X be a finite π-set and G a finite subgroup of $\mathrm{Aut}_{\pi\textbf{-sets}}(X)$. We define an action of π on X/G (the set of orbits of X under G, as in example 1.1.3(5)) as follows: $\sigma(Gx) = G(\sigma x)$ for any $\sigma \in \pi$, $x \in X$. Let us check that this is well defined. If $Gx_1 = Gx_2$, with $x_1, x_2 \in X$, there exists $g \in G$ such that $x_2 = gx_1$. Since g is a morphism of π-sets, we have that $\sigma x_2 = \sigma(gx_1) = g(\sigma x_1)$. Then $G(\sigma x_2) = G(\sigma x_1)$. This shows that $\sigma(Gx)$ is well defined for $Gx \in X/G$. We have that $1(Gx) = G(1x) = Gx$ and $(\sigma\tau)(Gx) = G((\sigma\tau)x) = G(\sigma(\tau x)) = \sigma(G(\tau x)) = \sigma(\tau(Gx))$, for any $Gx \in X/G$, $\sigma, \tau \in \pi$. So this is indeed a group action. Let us show that it is continuous. For any $Gx \in X/G$, we have that

$$\begin{aligned}\mathrm{Stab}_\pi(Gx) &= \{\sigma \in \pi \mid Gx = \sigma(Gx) = G(\sigma x)\} = \\ &= \{\sigma \in \pi \mid \exists g \in G \quad \sigma x = gx\} = \bigcup_{g \in G} \{\sigma \in \pi \mid \sigma x = gx\}\ .\end{aligned}$$

If we show that $U_{x,g} := \{\sigma \in \pi \mid \sigma x = gx\}$ is open in π for any $g \in G$, then $\mathrm{Stab}_\pi(Gx)$ is open. If $U_{x,g} = \emptyset$, then it is clearly open. Assume $U_{x,g} \neq \emptyset$. Then there exists $\sigma_0 \in U_{x,g}$. This means that $\sigma_0 x = gx$. We claim that $U_{x,g} = \sigma_0 \mathrm{Stab}_\pi(x)$. If $\sigma \in U_{x,g}$, we have that $\sigma x = gx = \sigma_0 x$. Then $(\sigma_0^{-1}\sigma)x = \sigma_0^{-1}(\sigma x) = x$. So $\sigma_0^{-1}\sigma \in \mathrm{Stab}_\pi(x)$. Then $\sigma \in \sigma_0 \mathrm{Stab}_\pi(x)$. Conversely, if $\sigma \in \sigma_0 \mathrm{Stab}_\pi(x)$, there exists $\tau \in \mathrm{Stab}_\pi(x)$ such that $\sigma = \sigma_0\tau$. Then $\sigma x = (\sigma_0\tau)x = \sigma_0(\tau x) = \sigma_0 x = gx$. So $\sigma \in U_{x,g}$. This shows that $U_{x,g} = \sigma_0 \mathrm{Stab}_\pi(x)$. Since the action of π on X is continuous, $\mathrm{Stab}_\pi(x)$ is open (see lemma 1.1.14). Since π is a topological group, left multiplication by σ_0 is a homeomorphism. So $U_{x,g}$ is open in π. By lemma 1.1.14, this shows that the action of π on X/G is continuous. We prove now that X/G, with this action and with the map $p : X \to X/G$ defined as in example 1.1.3(5), is the quotient of X by G in π-**sets**. First of all, p is a morphism of π-sets. Indeed, using the definition of p and of the action of π on X/G, we have that $p(\sigma x) = G(\sigma x) = \sigma(Gx) = \sigma p(x)$ for any $\sigma \in \pi$, $x \in X$. Moreover, $p = p \circ g$ for any $g \in G$ and, if Y is a finite π-set with a morphism of π-sets $f : X \to Y$ such that $f = f \circ g$ for any $g \in G$, we have a unique map $\overline{f} : X/G \to Y$ such that $\overline{f} \circ p = f$, as in example 1.1.3(5). We have to check that $\overline{f}$ is a morphism of π-sets. Since f is a morphism of π-sets, we have that

$$\overline{f}(\sigma(Gx)) = \overline{f}(G(\sigma x)) = f(\sigma x) = \sigma f(x) = \sigma\overline{f}(Gx)$$

for any $\sigma \in \pi$, $Gx \in X/G$. So $\overline{f}$ is a morphism of π-sets.

(G3) Let X, Y be finite π-sets and $u : X \to Y$ a morphism of π-sets. As in example 1.1.5, we can write $u = u' \circ u''$, with $u'' : X \to u(X)$ surjective and $u' : u(X) \to Y$ injective. If $y \in u(X)$, there exists $x \in X$ such that $y = u(x)$. Then, using the fact that u is a morphism of π-sets, we have $\sigma y = \sigma u(x) = u(\sigma x) \in u(X)$ for any $\sigma \in \pi$. So we can restrict the action of π from Y to $u(X)$. Clearly, the action of π on $u(X)$ is continuous, because the action on Y is continuous. So $u(X)$ is also a π-set. We have that u'' is

a morphism of π-sets because $u'' = u$ and the inclusion u' is a morphism of π-sets because the action of π on $u(X)$ is the restriction of that on Y. We have to check that u' and u'' are respectively a monomorphism and an epimorphism in π-**sets**. If Z is a finite π-set and $g, h : Z \to u(X)$ are two morphisms of π-sets such that $u' \circ g = u' \circ h$, then g and h are in particular maps of sets. By example 1.1.3(6), u' is a monomorphism in **sets**. So $g = h$. This shows that u' is a monomorphism in π-**sets**. Analogously, u'' is an epimorphism in **sets** by example 1.1.3(6) and so, if $g, h : u(X) \to Z$ are two morphisms of π-sets such that $g \circ u'' = h \circ u''$, we must have $g = h$. This shows that u'' is an epimorphism in π-**sets**.
Assume now that $u : X \to Y$ is a monomorphism in π-**sets**. We claim that u is injective. Let $x_1, x_2 \in X$ such that $u(x_1) = u(x_2)$. Let π' be the kernel of the action of π on X, as in lemma 1.1.14. Since the action of π is continuous, π' is open in π. By lemma 1.1.11, π' has finite index in π. So the set π/π' is finite. We have that π acts on π/π' by left multiplication: $\sigma(\tau\pi') = (\sigma\tau)\pi'$ for any $\sigma, \tau \in \pi$. This is well defined. Indeed, if $\tau_1\pi' = \tau_2\pi'$ for $\tau_1, \tau_2 \in \pi$, then $(\sigma\tau_2)^{-1}(\sigma\tau_1) = \tau_2^{-1}\tau_1 \in \pi'$. So $(\sigma\tau_1)\pi' = (\sigma\tau_2)\pi'$. This is clearly a group action. Moreover, it has kernel

$$\{\sigma \in \pi \mid \tau\pi' = \sigma(\tau\pi') = (\sigma\tau)\pi' \quad \forall \tau\pi' \in \pi/\pi'\} = \\ = \{\sigma \in \pi \mid \tau^{-1}\sigma\tau \in \pi' \quad \forall \tau \in \pi\} = \bigcap_{\tau \in \pi} \tau\pi'\tau^{-1} .$$

This is a finite intersection, because π' has finite index in π (notice that, if $\tau_1\pi' = \tau_2\pi'$ for $\tau_1, \tau_2 \in \pi$, then $\tau_1 = \tau_2\sigma$ for a $\sigma \in \pi'$ and so $\tau_1\pi'\tau_1^{-1} = \tau_2\sigma\pi'\sigma^{-1}\tau_2^{-1} = \tau_2\pi'\tau_2^{-1}$). Since π is a topological group, conjugation by τ is a homeomorphism for any $\tau \in \pi$. Then, since π' is open, $\tau\pi'\tau^{-1}$ is also open. So the kernel is open, because it is a finite intersection of open subsets. By lemma 1.1.14, the action of π on π/π' is continuous. So π/π' is a finite π-set. Define the functions $g : \pi/\pi' \to X$, $\tau\pi' \mapsto \tau x_1$ and $h : \pi/\pi' \to X$, $\tau\pi' \mapsto \tau x_2$. They are well defined. Indeed, if $\tau_1\pi' = \tau_2\pi'$, then $\tau_2 = \tau_1\sigma$, for a $\sigma \in \pi'$. Since π' is the kernel of the action of π on X, $\sigma x_1 = x_1$ and $\sigma x_2 = x_2$. Then $\tau_2 x_1 = (\tau_1\sigma)x_1 = \tau_1(\sigma x_1) = \tau_1 x_1$ and $\tau_2 x_2 = (\tau_1\sigma)x_1 = \tau_1(\sigma x_1) = \tau_1 x_1$. Moreover, if $\sigma \in \pi$ and $\tau\pi' \in \pi/\pi'$, then $g(\sigma(\tau\pi')) = g((\sigma\tau)\pi') = (\sigma\tau)x_1 = \sigma(\tau x_1) = \sigma g(\tau\pi')$ and $h(\sigma(\tau\pi')) = h((\sigma\tau)\pi') = (\sigma\tau)x_2 = \sigma(\tau x_2) = \sigma h(\tau\pi')$. So g and h are morphisms of π-sets. Since u is a morphism of π-sets and $u(x_1) = u(x_2)$, we have that

$$u(g(\tau\pi')) = u(\tau x_1) = \tau u(x_1) = \tau u(x_2) = u(\tau x_2) = u(h(\tau\pi'))$$

for any $\tau\pi' \in \pi/\pi'$. Then $u \circ g = u \circ h$. Since u is a monomorphism, this implies $g = h$. So $x_1 = g(\pi') = h(\pi') = x_2$. Hence u is injective. As above, we can restrict the action of π from Y to $u(X)$, which is then a finite π-set. On the other hand, if $y \in Y \backslash u(X)$, then $\sigma y \in Y \backslash u(X)$ for any $\sigma \in \pi$. Indeed, if we had $\sigma y \in u(X)$, we would have $y = \sigma^{-1}(\sigma y) \in u(X)$. So we can also restrict the action of π from Y to $Y \backslash u(X)$, obtaining a continuous action of π on $Y \backslash u(X)$, which is then a finite π-set. From the proof of (G2), it follows that $Y = u(X) \amalg (Y \backslash u(X))$, together with the natural inclusions, is the sum of $u(X)$ and $Y \backslash u(X)$ in **π-sets**. Let $q_2 : Y \backslash u(X) \to Y$ be the natural inclusion and $q_1 = u : X \to u(X)$. If we show that q_1 is an isomorphism of π-sets, then Y, together with q_1 and q_2, is the sum of X and $Z := Y \backslash u(X)$. Since u is injective, the map $q_1 = u : X \to u(X)$ is bijective. So it has an inverse $u^{-1} : u(X) \to X$. We have to show that u^{-1} is also a morphism of π-sets. Let $\sigma \in \pi$ and $y \in u(X)$. Then $y = u(u^{-1}(y))$. Since u is a morphism of π-sets, $\sigma y = \sigma u(u^{-1}(y)) = u(\sigma u^{-1}(y))$. So $u^{-1}(\sigma y) = \sigma u^{-1}(y)$. Then u^{-1} is a morphism of π-sets.

(G4) It follows from the proof of (G1) and from example 1.1.3(1)-(2).

(G5) The fact that F commutes with finite sums and with passage to the quotient by a finite group of automorphisms follows from the proof of (G2) and from example 1.1.3(3) and (5).
To show that F sends epimorphisms to epimorphisms, we have to check that any epimorphism of π-sets is a surjective map (see example 1.1.3(6)). Let X, Y be finite π-sets and $f : X \to Y$ an epimorphism. Consider the finite set $Z := \{a, b\}$, with $a \neq b$, and define on it the trivial action of π: $\sigma a = a$ and $\sigma b = b$, for any $\sigma \in \pi$. This is clearly a group action and it is continuous, because the associated map $\pi \times Z \to Z$ is just the projection on the second factor. Define the maps $g : Y \to Z$ and $h : Y \to Z$ as in example 1.1.3(6). Let $\sigma \in \pi$, $y \in Y$. Then $g(\sigma y) = a = \sigma a = \sigma g(y)$. So g is a morphism of π-sets. As in the proof of (G3), if $y \in f(X)$ then also $\sigma y \in f(X)$ and if $y \in Y \backslash f(X)$ then also $\sigma y \in Y \backslash f(X)$. In the first case, $h(\sigma y) = a = \sigma a = \sigma h(y)$. In the second case, $h(\sigma y) = b = \sigma b = \sigma h(y)$. Hence h is a morphism of π-sets. As in example 1.1.3(6), we have that $g \circ f = h \circ f$ and, since f is an epimorphism of π-sets, this implies $g = h$. So $Y = f(X)$, which means that f is surjective.

(G6) We have to show that, if X, Y are finite π-sets and $u : X \to Y$ is a bijective morphism of π-sets, then u is an isomorphism in **π-sets**. This can be done as in the proof of (G3).

□

1.2 Prorepresentability of F

In the next three sections, $\mathbf{C}$ will be an essentially small Galois category with fundamental functor F. Our aim is to prove that $\mathbf{C}$ is equivalent to the category **π-sets** for a (uniquely determined up to isomorphism) profinite group π. The first step will be to write F in a more convenient way, as an injective limit of functors of the form $\mathrm{Hom}_{\mathbf{C}}(A, -)$. We start by recalling the definition of injective limit (of sets).

Definition 1.2.1. An *injective system* of sets consists of a directed partially ordered set I, a collection of sets $(S_i)_{i \in I}$ and a collection of maps $(f_{ij} : S_i \to S_j)_{i,j \in I, i \leq j}$ such that

$$\forall i \in I \qquad f_{ii} = \mathrm{id}_{S_i}$$

and

$$\forall i,j,k \in I \text{ with } i \le j \le k \qquad f_{ik} = f_{jk} \circ f_{ij} \ .$$

Lemma 1.2.2. *Given an injective system of sets as in the definition 1.2.1, we define the following relation on the disjoint union $\coprod_{i\in I} S_i$: if $x \in S_i$ and $y \in S_j$ $(i,j \in I)$, then*

$$x \sim y \iff \exists k \in I : \quad k \ge i, k \ge j,\ f_{ik}(x) = f_{jk}(y) \ .$$

This relation is an equivalence relation.

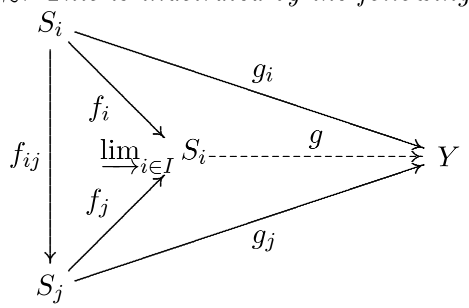
Proof. Let $x \in \coprod_{i\in I} S_i$. Then there exists $i \in I$ such that $x \in S_i$. We have that $i \ge i$ and clearly $f_{ii}(x) = f_{ii}(x)$. So $x \sim x$. Then $\sim$ is reflexive.
Let $x, y \in \coprod_{i\in I} S_i$ such that $x \sim y$. Then, if $i,j \in I$ are such that $x \in S_i$ and $y \in S_j$, there exists $k \in I$ such that $k \ge i$, $k \ge j$ and $f_{ik}(x) = f_{jk}(y)$. So $f_{jk}(y) = f_{ik}(x)$, which shows that $y \sim x$. Then $\sim$ is symmetric.
Let $x, y, z \in \coprod_{i\in I} S_i$ such that $x \sim y$ and $y \sim z$. Then, if $i,j,k \in I$ are such that $x \in S_i$, $y \in S_j$ and $z \in S_k$, there exist $h_1, h_2 \in I$ such that $h_1 \ge i$, $h_1 \ge j$ and $f_{ih_1}(x) = f_{jh_1}(y)$, $h_2 \ge j$, $h_2 \ge k$ and $f_{jh_2}(y) = f_{kh_2}(z)$. Since I is directed, there exists $h \in I$ such that $h \ge h_1$ and $h \ge h_2$. By definition of injective system, $f_{h_1h} \circ f_{ih_1} = f_{ih}$, $f_{h_1h} \circ f_{jh_1} = f_{jh} = f_{h_2h} \circ f_{jh_2}$ and $f_{h_2h} \circ f_{kh_2} = f_{kh}$. Then

$$f_{ih}(x) = f_{h_1h}(f_{ih_1}(x)) = f_{h_1h}(f_{jh_1}(y)) = f_{h_2h}(f_{jh_2}(y)) = f_{h_2h}(f_{kh_2}(z)) = f_{kh}(z) \ .$$

So $x \sim z$. Then $\sim$ is transitive. □

Definition 1.2.3. Given an injective system of sets as in the definition 1.2.1, the quotient $(\coprod_{i\in I} S_i)/\sim$, where $\sim$ is the equivalence relation defined in 1.2.2, is called the *injective limit* of the injective system and denoted with $\varinjlim_{i\in I} S_i$.

Lemma 1.2.4 (Universal property of the injective limit)**.** *Given an injective system of sets as in the definition 1.2.1, let Y be a set with a collection of maps $(g_j : S_j \to Y)_{j\in I}$ such that $g_i = g_j \circ f_{ij}$ for any $i,j \in I$ with $i \le j$. Then there exists a unique map $g : \varinjlim_{i\in I} S_i \to Y$ such that $g_j = g \circ f_j$ for any $j \in I$, where $f_j : S_j \to \varinjlim_{i\in I} S_i$ is defined by $f_j(x) = [x]_\sim$. This is illustrated by the following commutative diagram.*



Proof. (Existence) Let $X \in \varinjlim_{i\in I} S_i$. By definition of injective limit, there exist $j \in I$, $x \in S_j$ such that $X = [x]_\sim$. We define $g(X) = g_j(x) \in Y$. Let us check that this is well defined. Assume that $X = [x_1]_\sim = [x_2]_\sim$, with $x_1 \in S_{j_1}$, $x_2 \in S_{j_2}$ $(j_1, j_2 \in I)$. Then $x_1 \sim x_2$, which means that there exists $k \in I$ such that $k \geq j_1$, $k \geq j_2$ and $f_{j_1k}(x_1) = f_{j_2k}(x_2)$. By assumption, $g_{j_1} = g_k \circ f_{j_1k}$ and $g_{j_2} = g_k \circ f_{j_2k}$. Then

$$g_{j_1}(x_1) = g_k(f_{j_1k}(x_1)) = g_k(f_{j_2k}(x_2)) = g_{j_2}(x_2) \ .$$

This shows that $g : \varinjlim_{i\in I} Si \to Y$ is a well-defined map. Moreover, for any $j \in I$, $x \in S_j$, we have $(g \circ f_j)(x) = g(f_j(x)) = g([x]_\sim) = g_j(x)$. Hence $g \circ f_j = g_j$.

(Uniqueness) Consider a map $\widetilde{g} : \varinjlim_{i\in I} S_i \to Y$ such that $g_j = g \circ f_j$ for any $j \in I$. Let $X \in \varinjlim_{i\in I} S_i$. By definition of injective limit, there exist $j \in I$, $x \in S_j$ such that $X = [x]_\sim = f_j(x)$. Then $\widetilde{g}(X) = \widetilde{g}(f_j(x)) = (\widetilde{g} \circ f_j)(x) = g_j(x) = g(X)$. Hence $\widetilde{g} = g$.

□

Lemma 1.2.5. *If $I, (S_i)_{i\in I}, (f_{ij} : S_i \to S_j)_{i,j\in I, i\geq j}$ is a projective system in $\mathbf{C}$, then for any object X of $\mathbf{C}$ the collections $(\mathrm{Hom}_\mathbf{C}(S_i, X))_{i\in I}$, $(g_{ij} := f_{ji}^* : \mathrm{Hom}_\mathbf{C}(S_i, X) \to Hom_\mathbf{C}(S_j, X)$, $\varphi \mapsto \varphi \circ f_{ji})_{i,j\in I, i\leq j}$ form an injective system of sets.*

Proof. Let $i \in I$. Then $f_{ii} = \mathrm{id}_{S_i}$, by definition of projective system. So, for any $\varphi \in \mathrm{Hom}_\mathbf{C}(S_i, X)$, we have $f_{ii}^*(\varphi) = \varphi \circ f_{ii} = \varphi \circ \mathrm{id}_{S_i} = \varphi$. Then $g_{ii} = f_{ii}^* = \mathrm{id}_{\mathrm{Hom}_\mathbf{C}(S_i,X)}$. Let $i, j, k \in I$ such that $i \leq j \leq k$. By definition of projective system, $f_{ki} = f_{ji} \circ f_{kj}$. So, for any $\varphi \in \mathrm{Hom}_\mathbf{C}(S_i, X)$, we have $f_{ki}^*(\varphi) = \varphi \circ f_{ki} = \varphi \circ f_{ji} \circ f_{kj} = f_{ji}^*(\varphi) \circ f_{kj} = f_{kj}^*(f_{ji}^*(\varphi))$. Then $g_{ik} = f_{ki}^* = f_{kj}^* \circ f_{ji}^* = g_{jk} \circ g_{ij}$. □

Lemma 1.2.6. *If $I, (S_i)_{i\in I}, (f_{ij} : S_i \to S_j)_{i,j\in I, i\geq j}$ is a projective system in $\mathbf{C}$, then, by lemma 1.2.5, we can associate to each object X of $\mathbf{C}$ the injective limit $\varinjlim_{i\in I} \mathrm{Hom}_\mathbf{C}(S_i, X)$. Moreover, if X, Y are objects of $\mathbf{C}$ and $h : X \to Y$ is a morphism, we define*

$$\varinjlim_{i\in I} \mathrm{Hom}_\mathbf{C}(S_i, h) : \varinjlim_{i\in I} \mathrm{Hom}_\mathbf{C}(S_i, X) \to \varinjlim_{i\in I} \mathrm{Hom}_\mathbf{C}(S_i, Y),$$
$$\Phi = [\varphi]_\sim \mapsto [h \circ \varphi]_\sim \ .$$

Then $\varinjlim_{i\in I} \mathrm{Hom}_\mathbf{C}(S_i, -)$ is a functor.

Proof. First of all, we have to show that $\varinjlim_{i\in I} \mathrm{Hom}_\mathbf{C}(S_i, h)$ is well defined, for any morphism $h : X \to Y$ in $\mathbf{C}$. This follows from the universal property of the injective limit applied to the collection of maps $(\mathrm{Hom}_\mathbf{C}(S_j, X) \to \varinjlim_{i\in I} \mathrm{Hom}_\mathbf{C}(S_i, Y)$, $\varphi \mapsto [h \circ \varphi]_\sim)_{j\in I}$. We have only to check that these maps are compatible, i.e. that they satisfy the assumptions of lemma 1.2.4. Let $i, j \in I$ such that $i \leq j$ and let $\varphi \in \mathrm{Hom}_\mathbf{C}(S_i, X)$. Then

$$[h \circ g_{ij}(\varphi)]_\sim = [h \circ f_{ji}^*(\varphi)]_\sim = [h \circ \varphi \circ f_{ji}]_\sim = [f_{ji}^*(h \circ \varphi)]_\sim = [g_{ij}(h \circ \varphi)]_\sim \ .$$

We have that $g_{ij}(h\circ\varphi) = \mathrm{id}_{\mathrm{Hom}_\mathbf{C}(S_j,Y)}(g_{ij}(h\circ\varphi)) = g_{jj}(g_{ij}(h\circ\varphi))$. By definition of $\sim$ on $\coprod_{i\in I} \mathrm{Hom}_\mathbf{C}(S_i, Y)$, this implies that $h\circ\varphi \sim g_{ij}(h\circ\varphi)$. So $[h\circ g_{ij}(\varphi)]_\sim = [h\circ\varphi]_\sim$, as we wanted.

Let now X be an object of $\mathbf{C}$ and consider $h = \mathrm{id}_X : X \to X$. For any $\Phi = [\varphi]_\sim \in \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, X)$, we have that

$$\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, \mathrm{id}_X)(\Phi) = [\mathrm{id}_X \circ \varphi]_\sim = [\varphi]_\sim = \Phi \ .$$

Then $\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, \mathrm{id}_X) = \mathrm{id}_{\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, X)}$.
Let X, Y and Z be objects of $\mathbf{C}$, with two morphisms $h_1 : X \to Y$, $h_2 : Y \to Z$. For any $\Phi = [\varphi]_\sim \in \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, X)$, we have

$$\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h_2 \circ h_1)(\Phi) = [h_2 \circ h_1 \circ \phi]_\sim = \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h_2)([h_1 \circ \phi]_\sim) =$$
$$= \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h_2) \left(\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h_1)(\Phi) \right) \ .$$

Hence

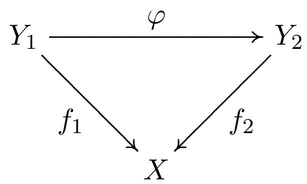
$$\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h_2 \circ h_1) = \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h_2) \circ \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h_1) \ .$$

□

Definition 1.2.7. A functor G from $\mathbf{C}$ to the category of (not necessarily finite) sets is called *prorepresentable* if there exists a projective system $I, (S_i)_{i\in I}, (f_{ij} : S_i \to S_j)_{i,j\in I, i\geq j}$ in $\mathbf{C}$ such that G is isomorphic to the functor $\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i, -)$ defined in lemma 1.2.6.

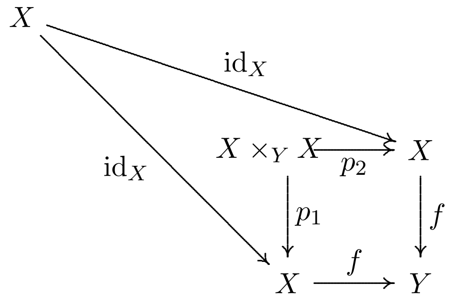
We want now to show that F is prorepresentable. To do it, we have to define a suitable projective system in $\mathbf{C}$.

Definition 1.2.8. A *subobject* of an object X of $\mathbf{C}$ is an equivalence class of monomorphisms $Y \to X$, where two monomorphisms $f_1 : Y_1 \to X$, $f_2 : Y_2 \to X$ are considered equivalent if and only if there exists an isomorphism $\varphi : Y_1 \to Y_2$ such that $f_1 = f_2 \circ \varphi$ (it is immediate to prove that this is an equivalence relation). The definition of this equivalence relation is illustrated by the following commutative diagram.

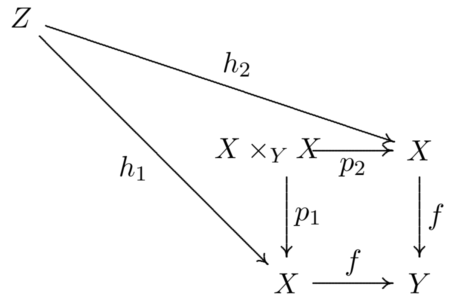


Lemma 1.2.9. *A morphism $f : X \to Y$ in $\mathbf{C}$ is a monomorphism if and only if the first projection $p_1 : X \times_Y X \to X$ is an isomorphism (remember that the fibred product exists by (G1) of the definition of Galois category).*

Proof. Consider the following diagram.



By definition of fibred product, there exists a unique morphism $g : X \to X \times_Y X$ such that $p_1 \circ g = \mathrm{id}_X$ and $p_2 \circ g = \mathrm{id}_X$.
Assume now that f is a monomorphism. Then, since $f \circ p_1 = f \circ p_2$, we must have $p_1 = p_2$. We have that $p_1 \circ g \circ p_1 = \mathrm{id}_X \circ p_1 = p_1 = p_1 \circ \mathrm{id}_{X \times_Y X}$ and $p_2 \circ g \circ p_1 = \mathrm{id}_X \circ p_1 = p_1 = p_2 = p_2 \circ \mathrm{id}_{X \times_Y X}$. By uniqueness in the universal property of the fibred product, this implies that $g \circ p_1 = \mathrm{id}_{X \times_Y X}$. This shows that g is the inverse of p_1 and so p_1 is an isomorphism.
Conversely, assume that p_1 is an isomorphism. Then, since $p_1 \circ g = \mathrm{id}_X$, we have that $g = p_1^{-1}$. Let $h_1, h_2 : Z \to X$ be morphisms such that $f \circ h_1 = f \circ h_2$. Consider the following diagram.



By the universal property of the fibred product, there exists a unique morphism $h : Z \to X \times_Y X$ such that $p_1 \circ h = h_1$ and $p_2 \circ h = h_2$. Then $h = p_1^{-1} \circ h_1 = g \circ h_1$ and $h_2 = p_2 \circ h = p_2 \circ g \circ h_1 = \mathrm{id}_X \circ h_1 = h_1$. Hence f is a monomorphism. □

Corollary 1.2.10. *If $f : X \to Y$ is a morphism in $\mathbf{C}$, then f is a monomorphism if and only if $F(f)$ is a monomorphism (i.e. if and only if $F(f)$ is injective, see example 1.1.3(6)).*

Proof. By lemma 1.2.9, f is a monomorphism if and only if the first projection $p_1 : X \times_Y X \to X$ is an isomorphism. By (G4) of the definition of Galois category, we have that $F(X \times_Y X)$ (together with $F(p_1)$, $F(p_2)$) is isomorphic to $F(X) \times_{F(Y)} F(X)$ (together with the canonical projections on $F(X)$). Then $F(f)$ is a monomorphism if and only if $F(p_1)$ is an isomorphism (by lemma 1.2.9 applied to the cateogry **sets**). By (G6) of the definition of Galois category, if $F(p_1)$ is an isomorphism then p_1 is also an isomorphism. The converse is true for any functor. Then p_1 is an isomorphism if and only if $F(p_1)$ is an isomorphism, which implies that f is a monomorphism if and only if $F(f)$ is a monomorphism. □

Example 1.2.11. (1) Recall that, by (G2) of the definition of Galois category, there exists an initial object 0 in $\mathbf{C}$. For any object X, the unique map $f : 0 \to X$

is a monomorphism. Indeed, by (G5) of the definition of Galois category, F commutes with finite sums. In particular, by remark 1.1.2(2), F sends an initial object of $\mathbf{C}$ to an initial object of **sets**. This means that $F(0) = \emptyset$ (see example 1.1.3(4)). Then $F(f) : \emptyset = F(0) \to F(X)$ is clearly injective. Hence, f is a monomorphism by corollary 1.2.10. If we consider two initial objects, the canonical isomorphism between them makes the diagram in the definition 1.2.8 commute, so they define the same subobject of X.

(2) For any object X, the identity $\mathrm{id}_X : X \to X$ is clearly a monomorphism. So it defines a subobject of X. Given a monomorphism $f : Y \to X$, it is equivalent to id_X if and only if there exists an isomorphism $\varphi : Y \to X$ such that $f = \mathrm{id}_X \circ \varphi = \varphi$, i.e. if and only if f is an isomorphism.

(3) If $X = 0$, the two subobjects considered in (1) and (2) coincide. On the other hand, if $f : Y \to 0$ is a monomorphism, then it is an isomorphism. Indeed, there exists a unique morphism $g : 0 \to Y$. Since id_0 is the unique morphism $0 \to 0$, we must have $f \circ g = \mathrm{id}_0$. Then we have also

$$f \circ (g \circ f) = (f \circ g) \circ f = \mathrm{id}_0 \circ f = f = f \circ \mathrm{id}_Y \ .$$

Since f is a monomorphism, this implies $g \circ f = \mathrm{id}_Y$. Then g is the inverse of f and f is an isomorphism. Hence, 0 has a unique subobject.
On the other hand, if $X \not\cong 0$, then X has at least two distinct subobjects, namely the ones considered in (1) and (2).

Definition 1.2.12. An object X of $\mathbf{C}$ is said *connected* if it has exactly two subobjects: $0 \to X$ and $X \xrightarrow{\mathrm{id}_X} X$.

Remark 1.2.13. (1) By definition, 0 is *not* a connected object, because it has only one subobject.

(2) In other words, X is connected if and only if, for every monomorphism $f : Y \to X$, either Y is initial or f is an isomorphism (but not both).

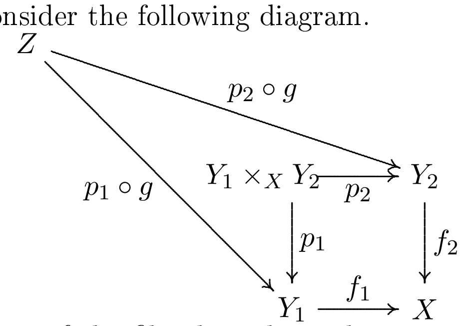
(3) Notice that connectedness is invariant by isomorphism, because, if $\varphi : X_1 \to X_2$ is an isomorphism, then composition with φ gives a bijection from subobjects of X_1 to subobjects of X_2 (the inverse being composition with φ^{-1}).

Example 1.2.14. (1) In the category **sets**, the connected objects are the singletons. Indeed, consider a singleton $\{x\}$ and a finite set Y with a monomorphism $f : Y \to X$. By example 1.1.3(6), f is injective. Then $|Y| \leq 1$. If $|Y| = 0$, then $Y = \emptyset$ is initial (example 1.1.3(4)). If $|Y| = 1$, then f is also surjective and so it is an isomorphism of sets. Hence $\{x\}$ is connected.
Conversely, assume X is a connected object. By remark 1.2.13(1), we have that $X \neq \emptyset$. Let $x \in X$. Then the natural inclusion $\iota : \{x\} \to X$ is injective, i.e. a monomorphism (example 1.1.3(4)). Since $\{x\} \neq \emptyset$, by remark 1.2.13(2) we must have that ι is an isomorphism, i.e. bijective. Then $X = \{x\}$ is a singleton.

(2) If π is a profinite group, the connected objects of the category π**-sets** are the finite sets with a transitive continuous action of π (recall that an action is called *transitive* if there is exactly one orbit, in particular the action on the empty set is not transitive).
Indeed, let X be a finite π-set on which the action of π is transitive. In particular, $X \neq \emptyset$. Let $f : Y \to X$ be a monomorphism of π-sets. Then f is injective, by corollary 1.2.10 (see also the proof of (G3) in proposition 1.1.15). Assume that $Y \neq \emptyset$. Then there exists $y \in Y$. Let $x \in X$. Since π acts transitively on X, there exists $\sigma \in \pi$ such that $x = \sigma f(y)$. Since f is a morphism of π-sets, we have that $\sigma f(y) = f(\sigma y)$. Then $x = f(\sigma y) \in f(Y)$. So f is surjective. We already knew that f was injective, so it is bijective, i.e. an isomorphism of sets. Since π**-sets** is a Galois category with fundamental functor the forgetful functor, by (G6) of the definition 1.1.4 this implies that f is an isomorphism of π-sets. Hence X is connected.
Conversely, assume that X is a connected object in π**-sets**. We can write X as the disjoint union of its orbits: $X = \coprod_{i=1}^{n} X_i$ ($n \in \mathbb{N}$). Since X is connected, by remark 1.2.13(1) we have that $X \neq \emptyset$. Then $n \geq 1$. We have that X_1 is a finite π-set and the natural inclusion $\iota : X_1 \to X$ is an injective morphism of π-sets, i.e. a monomorphism of π-sets (see corollary 1.2.10 or the proof of proposition 1.1.15). Since $X_1 \neq \emptyset$ (orbits are non-empty by definition) and X is connected, ι must be an isomorphism. Then $X \cong X_1$ and the action of π on X is transitive.

Lemma 1.2.15. *Let X, Y_1, Y_2 be objects of* $\mathbf{C}$ *and $f_1 : Y_1 \to X$, $f_2 : Y_2 \to X$ two morphisms. Consider the fibred product $Y_1 \times_X Y_2$ (whose existence is guaranteed by (G1) of the definition of Galois category), with the two projections $p_1 : Y_1 \times_X Y_2 \to Y_1$, $p_2 : Y_1 \times_X Y_2 \to Y_2$. If f_1 is a monomorphism, then p_2 is a monomorphism. If moreover f_2 is also a monomorphism, then $f_1 \circ p_1 = f_2 \circ p_2 : Y_1 \times_X Y_2 \to X$ is a monomorphism.*

Proof. Let Z be an object of $\mathbf{C}$, with two morphisms $g, h : Z \to Y_1 \times_X Y_2$ such that $p_2 \circ g = p_2 \circ h$. Then $f_2 \circ p_2 \circ g = f_2 \circ p_2 \circ h$. By definition of fibred product, $f_1 \circ p_1 = f_2 \circ p_2$. So $f_1 \circ p_1 \circ g = f_1 \circ p_1 \circ h$. Since f_1 is a monomorphism, this implies that $p_1 \circ g = p_1 \circ h$. Consider the following diagram.



By the universal property of the fibred product, there is a unique morphism $Z \to Y_1 \times_X Y_2$ making the diagram commute. Clearly g makes the diagram commute. Since $p_1 \circ g = p_1 \circ h$ and $p_2 \circ g = p_2 \circ h$, also h makes the diagram commute. Then $g = h$, which shows that p_2 is a monomorphism.
The last part of the statement follows from the fact that a composition of monomor-

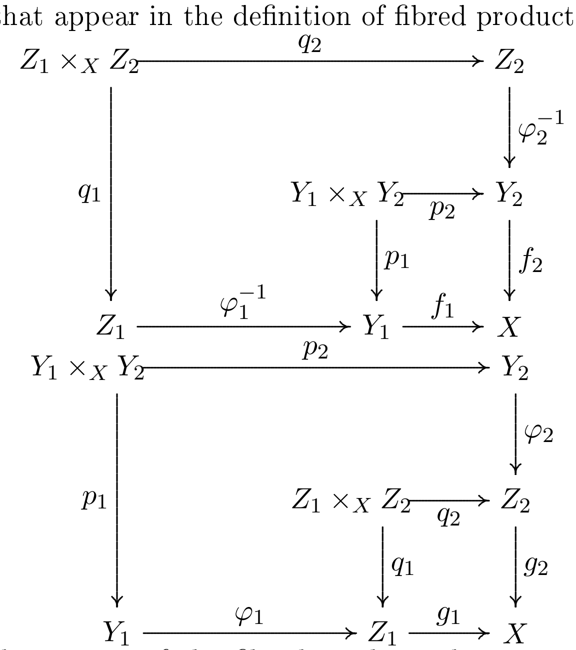
phisms is a monomorphism. □

Remark 1.2.16. (1) Let X be an object of $\mathbf{C}$. If $f : Y \to X$ is a monomorphism, then $F(f)$ is injective (corollary 1.2.10) and so we have

$$F(Y) \cong \mathrm{Im}(F(f)) \subseteq F(X) .$$

If $f_1 : Y_1 \to X$ and $f_2 : Y_2 \to X$ are two equivalent monomorphisms, then there exists an isomorphism $\varphi : Y_1 \to Y_2$ such that $f_1 = f_2 \circ \varphi$. Then $\mathrm{Im}(F(f_1)) = \mathrm{Im}(F(f_2 \circ \varphi)) = \mathrm{Im}(F(f_2))$ (in the last equality, we used the fact that $F(\varphi)$ is an isomorphism, i.e. a bijection). Hence any subobject of X gives rise to a subset of $F(X)$.

(2) Given two monomorphisms $f_1 : Y_1 \to X$ and $f_2 : Y_2 \to X$, consider the fibred product $Y_1 \times_X Y_2$, with the two projections $p_1 : Y_1 \times_X Y_2 \to Y_1$, $p_2 : Y_1 \times_X Y_2 \to Y_2$. By lemma 1.2.15, $f_1 \circ p_1 = f_2 \circ p_2 : Y_1 \times_X Y_2 \to X$ is a monomorphism. Moreover, if $g_1 : Z_1 \to X$ and $g_2 : Z_2 \to X$ are two other monomorphisms such that g_1 is equivalent to f_1 and g_2 is equivalent to f_2, then we have isomorphisms $\varphi_1 : Y_1 \to Z_1$, $\varphi_2 : Y_2 \to Z_2$ such that $f_1 = g_1 \circ \varphi_1$ and $f_2 = g_2 \circ \varphi_2$. Consider the following diagrams (where $q_1 : Z_1 \times_X Z_2 \to Z_1$, $q_2 : Z_1 \times_X Z_2 \to Z_2$ are the morphisms that appear in the definition of fibred product).



By the universal property of the fibred product, there exist morphisms $\varphi : Y_1 \times_X Y_2 \to Z_1 \times_X Z_2$, $\psi : Z_1 \times_X Z_2 \to Y_1 \times_X Y_2$ such that $q_1 \circ \varphi = \varphi_1 \circ p_1$, $q_2 \circ \varphi = \varphi_2 \circ p_2$, $p_1 \circ \psi = \varphi_1^{-1} \circ q_1$ and $p_2 \circ \psi = \varphi_2^{-1} \circ q_2$. Then

$$q_1 \circ \varphi \circ \psi = \varphi_1 \circ p_1 \circ \psi = \varphi_1 \circ \varphi_1^{-1} \circ q_1 = q_1 = q_1 \circ \mathrm{id}_{Z_1 \times_X Z_2}$$

and

$$q_2 \circ \varphi \circ \psi = \varphi_2 \circ p_2 \circ \psi = \varphi_2 \circ \varphi_2^{-1} \circ q_2 = q_2 = q_2 \circ \mathrm{id}_{Z_1 \times_X Z_2} .$$

By uniqueness in the universal property of the fibred product, we have that $\varphi \circ \psi = \mathrm{id}_{Z_1 \times_X Z_2}$. In the same way, one can show that $\psi \circ \varphi = \mathrm{id}_{Y_1 \times_X Y_2}$. So φ is an isomorphism. Moreover, $g_1 \circ q_1 \circ \varphi = g_1 = f_1 \circ p_1$. Then $f_1 \circ p_1 = f_2 \circ p_2 : Y_1 \times_X Y_2 \to X$ and $g_1 \circ q_1 = g_2 \circ q_2 : Z_1 \times_X Z_2 \to X$ are equivalent. In this way, we can use the fibred product to associate to every two subobjects of X another subobject, which we call their *intersection*. The reason of this name is that, by (G4) of the definition of Galois category, we have that $F(Y_1 \times_X Y_2)$ (together with $F(p_1)$ and $F(p_2)$) is isomorphic to $F(Y_1) \times_{F(X)} F(Y_2)$ (with the canonical projections). Then, recalling the definition of the fibred product of sets (example 1.1.3(2)), we have

$$\begin{aligned}\mathrm{Im}(F(f_1 \circ p_1)) = \mathrm{Im}(F(f_1) \circ F(p_1)) = \\ = \{x \in F(X) \mid \exists y \in \mathrm{Im}(F(p_1)) : F(f_1)(y) = x\} = \\ = \{x \in F(X) \mid \exists y \in F(Y_1), y' \in F(Y_2) : F(f_2)(y') = F(f_1)(y) = x\} = \\ = \mathrm{Im}(F(f_1)) \cap \mathrm{Im}(F(f_2)) \,.\end{aligned}$$

Assume now that $\mathrm{Im}(F(f_1)) = \mathrm{Im}(F(f_2))$, i.e. f_1 and f_2 give rise to the same subset of $F(X)$. Then $\mathrm{Im}(F(f_1 \circ p_1)) = \mathrm{Im}(F(f_1)) \cap \mathrm{Im}(F(f_2)) = \mathrm{Im}(F(f_1))$. So for any $y \in F(Y_1)$ there exists $z \in F(Y_1 \times_X Y_2)$ such that $F(f_1)(y) = F(f_1 \circ p_1)(z) = F(f_1)(F(p_1)(z))$. By corollary 1.2.10, $F(f_1)$ is a monomorphism, i.e. injective. Then $y = F(p_1)(z)$. So $F(p_1)$ is surjective. By corollary 1.2.10, $F(f_2)$ is a monomorphism. By lemma 1.2.15 applied to the category **sets** (exchanging the first and the second factor and recalling that by (G4) of the definition of Galois category F commutes with fibred product), $F(p_1)$ is also a monomorphism, i.e. injective. Hence $F(p_1)$ is a bijection, i.e. an isomorphism of sets. By (G6) of the definition of Galois category, p_1 is an isomorphism. In the same way, one can show that p_2 is an isomorphism. Then $p_2 \circ p_1^{-1} : Y_1 \to Y_2$ is an isomorphism. By definition of fibred product, $f_1 \circ p_1 = f_2 \circ p_2$. Then $f_1 = f_2 \circ (p_2 \circ p_1^{-1})$. This shows that f_1 and f_2 are equivalent.
In other words, to different subobjects of X must correspond different subsets of $F(X)$. In particular, since $F(X)$ is a finite set, X has finitely many subobjects.

Lemma 1.2.17. *Let X be an object of $\mathbf{C}$. If $F(X) = \emptyset$, then X is initial.*

Proof. By remark 1.2.16, the number of distinct subobjects of X is at most equal to the number of subsets $F(X)$. But $F(X) = \emptyset$ has a unique subset. So X has a unique subobject and, by example 1.2.11, this implies that $X \cong 0$. □

Definition 1.2.18. Let X be an object of $\mathbf{C}$. The *connected components* of X are its connected subobjects, i.e. the subobjects of the form $Y \to X$ with Y connected.

Lemma 1.2.19. *Let $X_1, \ldots, X_n$ be connected objects of $\mathbf{C}$ and consider their sum $X := \coprod_{i=1}^{n} X_i$, with the morphisms $q_1 : X_1 \to X, \ldots, q_n : X_n \to X$ as in the definition 1.1.1(3). Let Y be another connected object and $f : Y \to X$ a monomorphism. Then there exists a unique $i \in \{1, \ldots, n\}$ such that f is equivalent to q_i.*

Proof. Since Y is connected, Y is not initial (remark 1.2.13(1)). So $F(Y) \neq \emptyset$, by lemma 1.2.17. Then there exists $a \in F(Y)$. By (G5) of the definition of Galois category, we have that $F(X) = F(\coprod_{i=1}^n X_i) \cong \coprod_{i=1}^n F(X_i)$ (disjoint union of sets). Then, since $F(f)(a) \in F(X)$, there exists $i \in \{1, \dots, n\}$ such that $F(f)(a) \in \mathrm{Im}(F(q_i))$. Let us prove that f is equivalent to q_i. Consider the fibred product $Y \times_X X_i$. By lemma 1.2.15, the projections $p_1 : Y \times_X X_i \to Y$, $p_2 : Y \times_X X_i \to X_i$ are monomorphisms. Since Y and X_i are connected, this implies that either $Y \times_X X_i$ is initial or p_1 and p_2 are both isomorphisms. As in remark 1.2.16, we have that $\mathrm{Im}(F(f \circ p_1)) = \mathrm{Im}(F(f)) \cap \mathrm{Im}(F(q_i))$. Since $F(f)(a) \in \mathrm{Im}(F(q_i))$, we have that $F(f)(a) \in \mathrm{Im}(F(f)) \cap \mathrm{Im}(F(q_i)) = \mathrm{Im}(F(f \circ p_1))$. In particular, $\mathrm{Im}(F(f \circ p_1)) \neq \emptyset$. Then $F(Y \times_X X_i) \neq \emptyset$. By (G5) of the definition of Galois category, this implies that $Y \times_X X_i$ is not initial. Then p_1 and p_2 are both isomorphisms. So $p_2 \circ p_1^{-1} : Y \to X_i$ is an isomorphism and, by definition of fibred product, $q_i \circ p_2 \circ p_1^{-1} = f$. So f is equivalent to q_i.
Now we prove uniqueness. Assume that $i, j \in \{1, \dots, n\}$ are such that f is equivalent to both q_i and q_j. Then q_i is equivalent to q_j, which by remark 1.2.16 implies that $\mathrm{Im}(F(q_i)) = \mathrm{Im}(F(q_j))$. Since $F(X)$ is isomorphic to the disjoint union $\coprod_{i=1}^n F(X_i)$, we have that $\mathrm{Im}(F(q_i))$ and $\mathrm{Im}(F(q_j))$ are disjoint unless $i = j$. So $\mathrm{Im}(F(q_i)) = \mathrm{Im}(F(q_j))$ implies that $i = j$. □

Proposition 1.2.20. *Every object of* $\mathbf{C}$ *is the sum of its connected components.*

Proof. Let X be an object of $\mathbf{C}$. We prove the claim by induction on $n = |F(X)|$. If $|F(X)| = 0$, then $F(X) = \emptyset$. Then $X \cong 0$, by lemma 1.2.17. So X is the sum of the empty collection of objects (remark 1.1.2(2)). On the other hand, X has no connected subobjects (see example 1.2.11(3) and remark 1.2.13(1)). So X is the sum of its connected subobjects.
Assume the claim is true for every Y such that $|F(Y)| < n$. If X is connected, then its only connected subobject is $X \xrightarrow{id_X} X$. Clearly, $X = \coprod_{i=1}^1 X$, so the claim is true. If X is not connected, there exists a monomorphism $f : Y \to X$ such that Y is not initial and f is not an isomorphism. Then, by remark 1.2.16(2), $\mathrm{Im}(F(f)) \neq \emptyset$ and $\mathrm{Im}(F(f)) \neq F(X)$. This means that $0 < |\mathrm{Im}(F(f))| < n$. By corollary 1.2.10, $F(f)$ is injective. So $|F(Y)| = |\mathrm{Im}(F(f))|$. Then $0 < |F(Y)| < n$. By (G3) of the definition of Galois category, there exists an object Z and a morphism $q_2 : Z \to X$ such that X, together with $q_1 = f$ and q_2, is the sum of Y and Z. Then, by (G5) of the definition of Galois category and by example 1.1.3(3), $F(X)$, together with $F(f) : F(Y) \to F(X)$ and $F(q_2) : F(Z) \to F(X)$, is isomorphic to the disjoint union $F(Y) \amalg F(Z)$, together with the canonical inclusions. Notice that this implies that $F(q_2)$ is injective and so q_2 is a monomorphism by corollary 1.2.10. Moreover, $n = |F(X)| = |F(Y)| + |F(Z)|$. Since $|F(Y)| > 0$, we have $|F(Z)| < n$. Then we can apply induction to both Y and Z. In this way, we get $Y = \coprod_{i=1}^m Y_i$ and $Z = \coprod_{j=1}^p Z_j$, where $Y_1 \to Y, \dots, Y_m \to Y$ are the connected subobjects of Y and $Z_1 \to Z, \dots, Z_p \to Z$ are the connected subobjects of Z. Then $X = Y \amalg Z = (\coprod_{i=1}^m Y_i) \amalg (\coprod_{j=1}^p Z_j)$.
Since the composition of monomorphisms is a monomorphism, composition with f gives that $Y_1 \to X, \dots, Y_m \to X$ are connected subobjects of X and composition with

q_2 gives that $Z_1 \to X, \dots, Z_p \to X$ are connected subobjects of X. We claim that they are all the connected subobjects of X. Let $g : W \to X$ be a monomorphism, with W connected. Since $X = (\coprod_{i=1}^m Y_i) \amalg (\coprod_{j=1}^p Z_j)$ and $Y_1, \dots, Y_m$, $Z_1, \dots, Z_p$ are connected, we can apply lemma 1.2.19 to conclude that there exists either $i \in \{1, \dots, m\}$ such that g is equivalent to $Y_i \to X$ or $j \in \{1, \dots, p\}$ such that g is equivalent to $Z_j \to X$. □

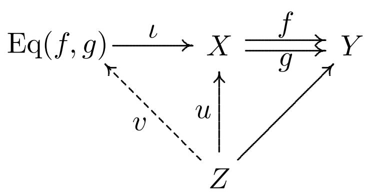
Corollary 1.2.21. *Let X be an object of $\mathbf{C}$ and $\sigma \in \mathrm{Aut}_{\mathbf{C}}(X)$. Then σ permutes the connected components of X, i.e., if $q_1 : X_1 \to X, \dots, q_n : X_n \to X$ are the (pairwise distinct) connected components of X, then for any $j \in \{1, \dots, n\}$ there exists a unique $j' \in \{1, \dots, n\}$ such that $\sigma \circ q_j$ is equivalent to $q_{j'}$.*

Proof. By proposition 1.2.20, we have that $X = \coprod_{i=1}^n X_i$. Let $j \in \{1, \dots, n\}$. Since composition of monomorphisms is a monomorphism, we have that $\sigma \circ q_j : X_j \to X = \coprod_{i=1}^n X_i$ is a monomorphism. Since $X_1, \dots, X_n$ are connected, we can apply lemma 1.2.19, which leads directly to the claim. □

Example 1.2.22. If π is a profinite group and X a finite π-set, then the decomposition of X in connected components coincides with its orbit decomposition, by example 1.2.14(2).

The proposition 1.2.20 is certainly useful to understand the objects of $\mathbf{C}$, because it reduces the problem of describing them to the problem of describing the connected objects. However, the first thing that we want to do with connected objects is to construct a projective system in $\mathbf{C}$, in order to show that F is prorepresentable. We will take into consideration pairs of the form (A, a), where A is a connected object of $\mathbf{C}$ and $a \in F(A)$, and use them to define a directed partially ordered set. Before doing it, we need to recall another notion in category theory.

Definition 1.2.23. Let X, Y be objects of $\mathbf{C}$, with two morphisms $f, g : X \to Y$. An *equalizer* of f and g is an object $\mathrm{Eq}(f, g)$ of $\mathbf{C}$, together with a morphism $\iota : \mathrm{Eq}(f, g) \to X$, such that $f \circ \iota = g \circ \iota$ and, for any object Z with a morphism $u : Z \to X$ satisfying $f \circ u = g \circ u$, there exists a unique morphism $v : Z \to \mathrm{Eq}(f, g)$ such that $u = \iota \circ v$. This definition is illustrated by the following commutative diagram.



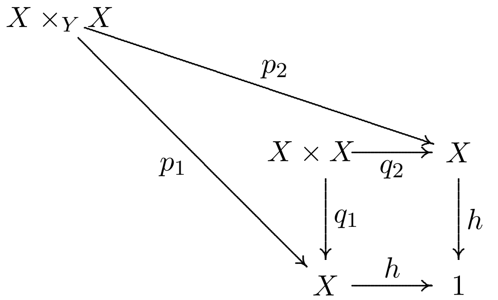
Remark 1.2.24. Being defined through a universal property, the equalizer of two morphisms, if it exists, is unique up to a unique isomomorphism.

Example 1.2.25. Let X, Y be finite sets, with two maps $f, g : X \to Y$. Set $W := \{x \in X \mid f(x) = g(x)\} \subseteq X$. Then W is a finite set. We claim that W, together with the canonical inclusion $\iota : W \to X$, is the equalizer of f and g in the category **sets** (notice that ι is injective, i.e. a monomorphism: we will show that this holds also in arbitrary categories). If $x \in W$, then by definition $f(\iota(x)) = f(x) = g(x) = g(\iota(x))$.

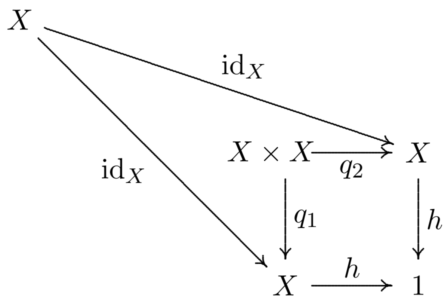
So $f \circ \iota = g \circ \iota$. Let Z be a finite set and $u : Z \to X$ a map such that $f \circ u = g \circ u$. Then, for any $z \in Z$, we have $f(u(z)) = g(u(z))$, which implies that $u(z) \in W$. So $u(Z) \subseteq W$. Then we can define $v = u : Z \to W$ and we have clearly that $u = \iota \circ v$. On the other hand, this is the unique possible definition if we want the diagram to commute.

Lemma 1.2.26. *Let X, Y be objects of $\mathbf{C}$, with two morphisms $f, g : X \to Y$. Consider the fibred product $X \times_Y X$, with projections $p_1 : X \times_Y X \to X$, $p_2 : X \times_Y X \to X$, and the product $X \times X = X \times_1 X$, with projections $q_1 : X \times X \to X$, $q_2 : X \times X \to X$ (both the product and the fibred product exist by (G1) of the definition of Galois category). There exist a morphism $p : X \times_Y X \to X \times X$ and a morphism $\Delta : X \to X \times X$ such that the fibred product $X \times_{X \times X} (X \times_Y X)$, together with the projection on the first factor, is an equalizer of f and g (again, this fibred product exists by (G1) of the definition of Galois category). In particular, any pair of morphisms admits an equalizer in the Galois category $\mathbf{C}$.*

Proof. Let $h : X \to 1$ be the unique morphisms from X to the terminal object 1. Since there is a unique morphism $X \times_Y X \to 1$, we have $h \circ p_1 = h \circ p_2$. Consider then the following diagram.



By the universal property of the fibred product, there exists a unique morphism $p : X \times_Y X \to X \times X$ such that $q_1 \circ p = p_1$ and $q_2 \circ p = p_2$. Consider now the following diagram.



By the universal property of the fibred product, there exists a unique morphism $\Delta : X \to X \times X$ such that $q_1 \circ \Delta = \mathrm{id}_X = q_2 \circ \Delta$. Let us consider the fibred product $X \times_{X \times X} (X \times_Y X)$ and let $\iota : X \times_{X \times X} (X \times_Y X) \to X$, $\kappa : X \times_{X \times X} (X \times_Y X) \to X \times_Y X$ be the two projections. By definition of fibred product, $\Delta \circ \iota = p \circ \kappa$. Then we have

$$\iota = \mathrm{id}_X \circ \iota = q_1 \circ \Delta \circ \iota = q_1 \circ p \circ \kappa = p_1 \circ \kappa$$

and

$$\iota = \mathrm{id}_X \circ \iota = q_2 \circ \Delta \circ \iota = q_2 \circ p \circ \kappa = p_2 \circ \kappa \, .$$

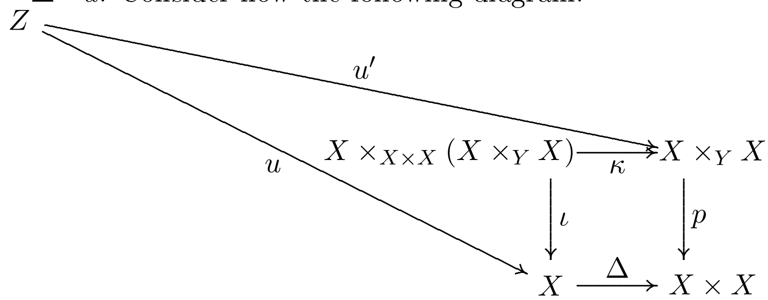
So, since $f \circ p_1 = g \circ p_2$ by definition of $X \times_Y X$, we have that $f \circ \iota = f \circ p_1 \circ \kappa = g \circ p_2 \circ \kappa = g \circ \iota$.
Moreover, let Z be an object of $\mathbf{C}$ with a morphism $u : Z \to X$ such that $f \circ u = g \circ u$. By the universal property of the fibred product $X \times_Y X$, there exists a unique $u' : Z \to X \times_Y X$ such that $p_1 \circ u' = u = p_2 \circ u'$. We have that

$$q_1 \circ p \circ u' = p_1 \circ u' = u = \mathrm{id}_X \circ u = q_1 \circ \Delta \circ u$$

and

$$q_2 \circ p \circ u' = p_2 \circ u' = u = \mathrm{id}_X \circ u = q_2 \circ \Delta \circ u \, .$$

By uniqueness in the universal property for the product $X \times X = X \times_1 X$, we must have $p \circ u' = \Delta \circ u$. Consider now the following diagram.



By the universal property of the fibred product, there exists a unique $v : Z \to X \times_{X \times X} (X \times_Y X)$ such that $\iota \circ v = u$ and $\kappa \circ v = u'$.
To conclude, let $\widetilde{v} : Z \to X \times_{X \times X} (X \times_Y X)$ be such that $\iota \circ \widetilde{v} = u$. Then $p_1 \circ \kappa \circ \widetilde{v} = \iota \circ \widetilde{v} = u$ and $p_2 \circ \kappa \circ \widetilde{v} = \iota \circ \widetilde{v} = u$. By uniqueness of u', this implies $\kappa \circ \widetilde{v} = u'$. Hence $\widetilde{v} = v$. □

Corollary 1.2.27. *F commutes with equalizers.*

Proof. It follows by (G4) of the definition of Galois category and by lemma 1.2.26 (applied to both $\mathbf{C}$ and **sets**), since p and Δ were constructed using the universal property of the fibred product. □

Lemma 1.2.28. *Let X, Y be objects of $\mathbf{C}$, with two morphisms $f, g : X \to Y$. Consider the equalizer $\mathrm{Eq}(f, g)$, together with the morphism $\iota : \mathrm{Eq}(f, g) \to X$, as in the definition. Then ι is a monomorphism.*

Proof. Let Z be an object of $\mathbf{C}$, with two morphisms $h_1, h_2 : Z \to \mathrm{Eq}(f, g)$ such that $\iota \circ h_1 = \iota \circ h_2$. Since $f \circ \iota = g \circ \iota$, we have that $f \circ \iota \circ h_1 = g \circ \iota \circ h_1$. Then, by the universal property of the equalizer, there exists a unique morphism $h : Z \to \mathrm{Eq}(f, g)$ such that $\iota \circ h = \iota \circ h_1$. This implies $h_1 = h_2$. □

Corollary 1.2.29. *Let A, X be objects of $\mathbf{C}$, with A connected, and let $f, g : A \to X$ be two morphisms. Then $\mathrm{Eq}(f, g)$ is initial or $f = g$.*

Proof. By lemma 1.2.28, $\iota : \mathrm{Eq}(f, g) \to A$ is a monomorphism. By definition of connected objects, this implies that either $\mathrm{Eq}(f, g)$ is initial or ι is an isomorphism. In the last case, we have

$$f = f \circ \mathrm{id}_A = f \circ \iota \circ \iota^{-1} = g \circ \iota \circ \iota^{-1} = g \circ \mathrm{id}_A = g$$

($f \circ \iota = g \circ \iota$ by definition of equalizer). □

Lemma 1.2.30. *Let A be a connected object of $\mathbf{C}$ and $a \in F(A)$. For any object X of $\mathbf{C}$, define the map*

$$\psi^X_{(A,a)} : \mathrm{Hom}_{\mathbf{C}}(A, X) \to F(X),\ f \mapsto F(f)(a)\ .$$

Then $\psi^X_{(A,a)}$ is injective.

Proof. Let $f, g \in \mathrm{Hom}_{\mathbf{C}}(A, X)$ such that $\psi^X_{(A,a)}(f) = \psi^X_{(A,a)}(g)$. This means that $F(f)(a) = F(g)(a)$. Then $a \in \mathrm{Eq}(F(f), F(g)) \subseteq F(A)$ (see example 1.2.25). In particular, $\mathrm{Eq}(F(f), F(g)) \neq \emptyset$. By corollary 1.2.27, we have that $\mathrm{Eq}(F(f), F(g)) \cong F(\mathrm{Eq}(f, g))$. So $F(\mathrm{Eq}(f, g)) \neq \emptyset$ and, by (G5) of the definition of Galois category, this implies that $\mathrm{Eq}(f, g)$ is not initial. Since A is connected, by corollary 1.2.29 we must have $f = g$. Hence $\psi^X_{(A,a)}$ is injective. □

Lemma 1.2.31. *Let $\mathcal{I} := \{(A, a) \mid A$ connected, $a \in F(A)\}$. We define the following relation on $\mathcal{I}$:*

$$(A, a) \geq (B, b) \iff \exists f \in \mathrm{Hom}_{\mathbf{C}}(A, B) : b = F(f)(a)\ .$$

This relation is a preorder, i.e. it is reflexive and transitive. Moreover, $(A, a) \geq (B, b)$ and $(B, b) \geq (A, a)$ if and only if there exists an isomorphism $f : A \to B$ such that $b = F(f)(a)$. In this case we write $(A, a) \sim (B, b)$. Then we have an induced order relation on the quotient $\mathcal{I}/\sim$. Denote this quotient with I. Then I is a directed partially ordered set.

Proof. Let $(A, a) \in \mathcal{I}$ and consider $\mathrm{id}_A \in \mathrm{Hom}_{\mathbf{C}}(A, A)$. Since F is a functor, $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$. Then $a = \mathrm{id}_{F(A)}(a) = F(\mathrm{id}_A)(a)$. This shows that $(A, a) \geq (A, a)$ and so $\geq$ is reflexive.
Let $(A, a), (B, b), (C, c) \in \mathcal{I}$ such that $(A, a) \geq (B, b)$ and $(B, b) \geq (C, c)$. Then there exist $f \in \mathrm{Hom}_{\mathbf{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathbf{C}}(B, C)$ such that $F(f)(a) = b$ and $F(g)(b) = c$. We have that $g \circ f \in \mathrm{Hom}_{\mathbf{C}}(A, C)$ and, since F is a functor, $F(g \circ f) = F(g) \circ F(f)$. So $F(g \circ f)(a) = F(g)(F(f)(a)) = F(g)(b) = c$. This shows that $(A, a) \geq (C, c)$ and so $\geq$ is transitive.
Assume that $(A, a), (B, b) \in \mathcal{I}$ are such that $(A, a) \geq (B, b)$ and $(B, b) \geq (A, a)$. Then there exist $f \in \mathrm{Hom}_{\mathbf{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathbf{C}}(B, A)$ such that $F(f)(a) = b$ and $F(g)(b) = a$. We have that $g \circ f \in \mathrm{Hom}_{\mathbf{C}}(A, A)$ and $F(g \circ f)(a) = F(g)(F(f)(a)) = F(g)(b) = a = F(\mathrm{id}_A)(a)$. This means that $\psi^X_{(A,a)}(g \circ f) = \psi^X_{(A,a)}(\mathrm{id}_A)$, which by lemma 1.2.30 implies that $g \circ f = \mathrm{id}_A$. Analogously, one can show that $f \circ g = id_B$. So f and g are inverse to each other. In particular, f is an isomorphism.
Conversely, assume that $(A, a), (B, b) \in \mathcal{I}$ and there exists an isomorphism $f : A \to B$ with $b = F(f)(a)$. Clearly, this implies that $(A, a) \geq (B, b)$. Moreover, we have that $f^{-1} \in \mathrm{Hom}_{\mathbf{C}}(B, A)$ and $F(f^{-1}) = F(f)^{-1}$. So $F(f^{-1})(b) = F(f)^{-1}(b) = a$. This shows that $(B, b) \geq (A, a)$.
The last thing that we have to prove is that I is a directed partially ordered set. First of all, I is a set because $\mathbf{C}$ is essentially small (on the other hand, $\mathcal{I}$ could be a proper class).
Let $[(A, a)]_\sim, [(B, b)]_\sim \in I$. Consider the product $A \times B = A \times_1 B$. By proposition 1.2.20, we can write $A \times B = \coprod_{i=1}^n C_i$, with each C_i connected (with morphisms

$q_j : C_j \to A \times B$ for any $j = 1, \dots, n$, as in the definition 1.1.1(3)). By (G4) of the definition of Galois category, there exists an isomorphism $\varphi : F(A) \times F(B) \to F(A \times B)$ such that $p'_1 = F(p_1) \circ \varphi$ and $p'_2 = F(p_2) \circ \varphi$, where $p_1 : A \times B \to A$, $p_2 : A \times B \to B$, $p'_1 : F(A) \times F(B) \to F(A)$, $p'_2 : F(A) \times F(B) \to F(B)$ are the projections. Consider now $(a, b) \in F(A) \times F(B)$. Then $\varphi((a, b)) \in F(A \times B)$. By (G5) of the definition of Galois category, $F(A \times B) = F(\coprod_{i=1}^n C_i) \cong \coprod_{i=1}^n F(C_i)$ (disjoint union, see example 1.1.3(3)) and the isomorphism is compatible with the inclusions. So there exists a unique $j \in \{1, \dots, n\}$ such that $\varphi((a, b)) \in \mathrm{Im}(F(q_j))$. Let $c \in F(C_j)$ be such that $\varphi((a, b)) = F(q_j)(c)$. Then we have

$$F(p_1 \circ q_j)(c) = F(p_1)(F(q_j)(c)) = F(p_1)(\varphi((a, b))) = p'_1((a, b)) = a$$

and

$$F(p_2 \circ q_j)(c) = F(p_2)(F(q_j)(c)) = F(p_2)(\varphi((a, b))) = p'_2((a, b)) = b\ .$$

This shows that $(C_j, c) \geq (A, a)$ and $(C_j, c) \geq (B, b)$. Then $[(C_j, c)]_\sim \geq [(A, a)]_\sim$ and $[(C_j, c)]_\sim \geq [(B, b)]_\sim$. Hence I is directed. □

Remark 1.2.32. (1) While the definition of connected object is independent of the functor F, we have that $\mathcal{I}$ and I depend on F, because on the one hand an element of $\mathcal{I}$ is identified not only by a connected object A, but also by an element $a \in F(A)$, and on the other hand also the relation defined in lemma 1.2.31 depends on F.

(2) Let $(A, a), (B, b) \in \mathcal{I}$ and $(A, a) \geq (B, b)$. By definition, this means that there exists $f : A \to B$ such that $b = F(f)(a)$. Assume that $f' : A \to B$ is another morphism such that $b = F(f')(a)$. Then $\psi^X_{(A,a)}(f) = F(f)(a) = b = F(f')(a) = \psi^X_{(A,a)}(f')$, which by lemma 1.2.30 implies that $f = f'$. So the morphism f that appears in the definition of $\geq$ is uniquely determined.

Lemma 1.2.33. *Let I be defined as in lemma 1.2.31. For any $i \in I$, choose a pair $(A_i, a_i) \in \mathcal{I}$ such that $i = [(A_i, a_i)]_\sim$. For any $i, j \in I$ such that $i \geq j$ (i.e. $(A_i, a_i) \geq (A_j, a_j)$), let $f_{ij} : A_i \to A_j$ be the unique morphism such that $F(f_{ij})(a_i) = a_j$ (see remark 1.2.32(2)). Then $(A_i)_{i \in I}, (f_{ij} : A_i \to A_j)_{i,j \in I, i \geq j}$ is a projective system in* $\mathbf{C}$.

Proof. For any $i \in I$, we have $F(\mathrm{id}_{A_i})(a_i) = a_i$ (because F is a functor). By uniqueness, this implies that $f_{ii} = id_{A_i}$.
Let $i, j, k \in I$ such that $i \geq j \geq k$. Since F is a functor, we have that

$$F(f_{jk} \circ f_{ij})(a_i) = F(f_{jk})(F(f_{ij})(a_i)) = F(f_{jk})(a_j) = a_k\ .$$

By uniqueness, this implies that $f_{ik} = f_{jk} \circ f_{ij}$. □

Remark 1.2.34. In lemma 1.2.33, we made a choice in order to define a projective system. So this projective system is not uniquely determined. However, the choice does not affect the functor $\varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, -)$, which is what we are interested in. Indeed, if for any $i \in I$ we choose $(B_i, b_i) \in \mathcal{I}$ such that $i = [(B_i, b_i)]_\sim$, then there exists a unique isomorphism $\varphi_i : B_i \to A_i$ such that $F(\varphi_i)(b_i) = a_i$. This isomorphism gives rise to a bijection

$$\varphi_i^* : \mathrm{Hom}_{\mathbf{C}}(A_i, X) \to \mathrm{Hom}_{\mathbf{C}}(B_i, X),\ f \mapsto f \circ \varphi_i \ ,$$

for any object X of $\mathbf{C}$. Moreover, if $i, j \in I$ and $i \geq j$, we have that $g_{ij} := \varphi_j^{-1} \circ f_{ij} \circ \varphi_i$ is the unique morphism $B_i \to B_j$ such that $F(g_{ij})(b_i) = b_j$. So the following diagram is commutative.

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathbf{C}}(A_i, X) & \xrightarrow{\varphi_i^*} & \mathrm{Hom}_{\mathbf{C}}(B_i, X) \\
{\scriptstyle f_{ij}^*}\uparrow & & \uparrow{\scriptstyle g_{ij}^*} \\
\mathrm{Hom}_{\mathbf{C}}(A_j, X) & \xrightarrow{\varphi_j^*} & \mathrm{Hom}_{\mathbf{C}}(B_j, X)
\end{array}$$

At this point, one can use the universal property of the injective limit to "glue" together the bijections φ_i^* and get a bijection

$$\Phi_X : \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, X) \to \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(B_i, X) \ .$$

If X, Y are two objects of $\mathbf{C}$ and $h : X \to Y$ is a morphism, then it can be proved that $\Phi_Y \circ \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, h) = \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(B_i, X) \circ \Phi_X$. This shows that the functors $\varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, -)$ and $\varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(B_i, -)$ are isomorphic.

Proposition 1.2.35. *F is isomorphic to the functor $\varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, -)$, where the projective system is the one defined in lemma 1.2.33. In particular, F is prorepresentable.*

Proof. Let X be an object of $\mathbf{C}$. For any $i \in I$, consider the map $\psi^X_{(A_i, a_i)}$, as defined in lemma 1.2.30. Let $i, j \in I$ such that $i \geq j$. For any $f \in \mathrm{Hom}_{\mathbf{C}}(A_j, X)$, we have that

$$\left(\psi^X_{(A_i,a_i)} \circ f_{ij}^*\right)(f) = \psi^X_{(A_i,a_i)}(f \circ f_{ij}) = F(f \circ f_{ij})(a_i) = \\ = F(f)(F(f_{ij})(a_i)) = F(f)(a_j) = \psi^X_{(A_j,a_j)}(f) \ .$$

Then $\psi^X_{(A_i,a_i)} \circ f_{ij}^* = \psi^X_{(A_j,a_j)}$. By the universal property of the injective limit (lemma 1.2.4), there exists a unique map $\psi^X : \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, X) \to F(X)$ such that $\psi^X_{(A_j,a_j)} = \psi^X \circ f_j^X$ for any $j \in I$, where $f_j^X : \mathrm{Hom}_{\mathbf{C}}(A_j, X) \to \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, X)$ is defined by $f_j^X(g) = [g]_\sim$. We claim that ψ^X is bijective.
Let $[g_1]_\sim, [g_2]_\sim \in \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, X)$ such that $\psi^X([g_1]_\sim) = \psi^X([g_2]_\sim)$. Then there exist $i, j \in I$ such that $g_1 \in \mathrm{Hom}_{\mathbf{C}}(A_i, X)$, $g_2 \in \mathrm{Hom}_{\mathbf{C}}(A_j, X)$. Since I is directed, there exists $k \in I$ such that $k \geq i$ and $k \geq j$. Then

$$\psi^X_{(A_k,a_k)}(f_{ik}(g_1)) = \psi^X(f_k^X(f_{ik}(g_1))) = \psi^X([f_{ik}(g_1)]_\sim) = \psi^X([g_1]_\sim) = \\ = \psi^X([g_2]_\sim) = \psi^X([f_{jk}(g_2)]_\sim) = \psi^X(f_k^X(f_{jk}(g_2))) = \psi^X_{(A_k,a_k)}(f_{jk}(g_2)) \ .$$

But we know that $\psi^X_{(A_k,a_k)}$ is injective (lemma 1.2.30). So we must have $f_{ik}(g_1) = f_{jk}(g_2)$, which implies that $g_1 \sim g_2$. Hence $[g_1]_\sim = [g_2]_\sim$ and ψ^X is injective.

Let $x \in F(X)$. By proposition 1.2.20, we have $X = \coprod_{\alpha=1}^{n} X_\alpha$, where $q_1 : X_1 \to X, \dots, q_n : X_n \to X$ are the connected components of X. By (G5) of the definition of Galois category, $F(X) \cong \coprod_{\alpha=1}^{n} F(X_\alpha)$ and the isomorphism is compatible with inclusions. Then there exists a unique $\beta \in \{1, \dots, n\}$ such that $x \in \mathrm{Im}(F(q_\beta))$. So there exists $a \in F(X_\beta)$ such that $x = F(q_\beta)(a)$. Since X_β is connected, we have that $(X_\beta, a) \in \mathcal{I}$. Set $j := [(X_\beta, a)]_\sim \in I$. Then $(X_\beta, a) \sim (A_j, a_j)$, i.e. we have an isomorphism $f : A_j \to X_\beta$ such that $F(f)(a_j) = a$. Then $q_\beta \circ f \in \mathrm{Hom}_{\mathbf{C}}(A_j, X)$ and

$$\psi^X_{(A_j,a_j)}(q_\beta \circ f) = F(q_\beta \circ f)(a_j) = F(q_\beta)(F(f)(a_j)) = F(q_\beta)(a) = x \; .$$

Hence $[q_\beta \circ f]_\sim \in \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(A_i, X)$ and $\psi^X([q_\beta \circ f]_\sim) = \psi^X(f_j^X(q_\beta \circ f)) = \psi^X_{(A_j,a_j)}(q_\beta \circ f) = x$. This shows that ψ^X is surjective.

It remains to prove that the bijections ψ^X's are compatible with morphisms. Let X, Y be objects of $\mathbf{C}$ and $h : X \to Y$ a morphism. Let $i \in I$ and consider the following diagram.

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{C}}(A_i, X) & \xrightarrow{\psi^X_{(A_i,a_i)}} & F(X) \\ {\scriptstyle h\circ -}\downarrow & & \downarrow{\scriptstyle F(h)} \\ \mathrm{Hom}_{\mathbf{C}}(A_i, Y) & \xrightarrow{\psi^Y_{(A_i,a_i)}} & F(Y) \end{array}$$

For any $g \in \mathrm{Hom}_{\mathbf{C}}(A_i, X)$, we have that

$$\left(F(h) \circ \psi^X_{(A_i,a_i)}\right)(g) = F(h)\left(\psi^X_{(A_i,a_i)}(g)\right) = F(h)(F(g)(a_i)) = \\ = F(h \circ g)(a_i) = \psi^Y_{(A_i,a_i)}(h \circ g) \; .$$

Hence the diagram is commutative. Now we work with the limit. We have to show that $F(h) \circ \psi^X = \psi^Y \circ \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(A_i, h)$. By uniqueness in the universal property of the injective limit, it is enough to prove that $F(h) \circ \psi^X \circ f_j^X = \psi^Y \circ \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(A_i, h) \circ f_j^X$ for any $j \in I$. Let $g \in \mathrm{Hom}_{\mathbf{C}}(A_j, X)$. By definition, we have that $\left(\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(A_i, h) \circ f_j^X\right)(g) = [h \circ g]_\sim$ (see lemma 1.2.6). Then, by what we proved above, we have

$$\left(\psi^Y \circ \varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(A_i, h) \circ f_j^X\right)(g) = \psi^Y([h \circ g]_\sim) = \psi^Y\left(f_j^Y(h \circ g)\right) = \\ = \psi^Y_{(A_j,a_j)}(h \circ g) = \left(F(h) \circ \psi^X_{(A_j,a_j)}\right)(g) = \left(F(h) \circ \psi^X \circ f_j^X\right)(g) \; .$$

This ends the proof. □

1.3 A profinite group

Now that we have a very concrete description of the functor F, the next step is to define a profinite group which acts in a natural way on $F(X)$ for any object X.

Definition 1.3.1. An object A of $\mathbf{C}$ is called a *Galois object* if it is connected and $A/\operatorname{Aut}_{\mathbf{C}}(A)$ is terminal.

Remark 1.3.2. (1) For any connected object A of $\mathbf{C}$, lemma 1.2.30 implies that $|\operatorname{Hom}_{\mathbf{C}}(A,A)| \leq |F(A)|$. Then, since $\operatorname{Aut}_{\mathbf{C}}(A)$ is a subset of $\operatorname{Hom}_{\mathbf{C}}(A,A)$, we have that

$$|\operatorname{Aut}_{\mathbf{C}}(A)| \leq |\operatorname{Hom}_{\mathbf{C}}(A,A)| \leq |F(A)| \,.$$

In particular, $\operatorname{Aut}_{\mathbf{C}}(A)$ is finite, because $F(A)$ is finite. Then the quotient $A/\operatorname{Aut}_{\mathbf{C}}(A)$ exists by (G2) of the definition of Galois category. Hence the definition 1.3.1 makes sense.

(2) The property of being a Galois object is invariant by isomorphism. Indeed, assume that $\varphi : A \to B$ is an isomorphism and A is Galois. In particular, A is connected and this implies that B is also connected (see remark 1.2.13(3)). Denote by $p_A : A \to A/\operatorname{Aut}_{\mathbf{C}}(A)$ and $p_B : B \to B/\operatorname{Aut}_{\mathbf{C}}(B)$ the morphisms that appear in the definition of the quotient (see definition 1.1.1(5)). Let $\sigma \in \operatorname{Aut}_{\mathbf{C}}(A)$. Then $\varphi \circ \sigma \circ \varphi^{-1} \in \operatorname{Aut}_{\mathbf{C}}(B)$. So, by definition of quotient, $p_B \circ \varphi \circ \sigma \circ \varphi^{-1} = p_B$. Hence $(p_B \circ \varphi) \circ \sigma = p_B \circ \varphi$. Since this holds for any $\sigma \in \operatorname{Aut}_{\mathbf{C}}(A)$, by the universal property of the quotient there exists a unique morphism $\Phi : A/\operatorname{Aut}_{\mathbf{C}}(A) \to B/\operatorname{Aut}_{\mathbf{C}}(B)$ such that $p_B \circ \varphi = \Phi \circ p_A$. In the same way, one can show that there exists a unique morphism $\Psi : B/\operatorname{Aut}_{\mathbf{C}}(B) \to A/\operatorname{Aut}_{\mathbf{C}}(A)$ such that $p_A \circ \varphi^{-1} = \Psi \circ p_B$. Then

$$(\Psi \circ \Phi) \circ p_A = \Psi \circ p_B \circ \varphi = p_A \circ \varphi^{-1} \circ \varphi = p_A = \operatorname{id}_{A/\operatorname{Aut}_{\mathbf{C}}(A)} \circ p_A \,.$$

By uniqueness in the universal property of the quotient, this implies $\Psi \circ \Phi = \operatorname{id}_{A/\operatorname{Aut}_{\mathbf{C}}(A)}$. Analogously, $\Phi \circ \Psi = \operatorname{id}_{B/\operatorname{Aut}_{\mathbf{C}}(B)}$. So $A/\operatorname{Aut}_{\mathbf{C}}(A) \cong B/\operatorname{Aut}_{\mathbf{C}}(B)$. Since A is Galois, $A/\operatorname{Aut}_{\mathbf{C}}(A)$ is terminal. Hence $B/\operatorname{Aut}_{\mathbf{C}}(B)$ is also terminal, i.e. B is Galois.

(3) The definition of Galois object does not depend on the functor F.

Lemma 1.3.3. *Let X be an object of $\mathbf{C}$. Then $|F(X)| = 1$ if and only if X is terminal.*

Proof. By (G4) of the definition of Galois category, if X is terminal then $F(X)$ is also terminal, i.e. a singleton (example 1.1.3(1)).
Conversely, assume that $|F(X)| = 1$, i.e. $F(X)$ is a singleton. Let $f : X \to 1$ be the unique morphism from X to the terminal object. Consider the map $F(f) : F(X) \to F(1)$. By (G4) of the definition of Galois category, $F(1)$ is a singleton. Then $F(f)$ is a map from a singleton to another singleton. So $F(f)$ must be a bijection, i.e. an isomorphism of sets. By (G6) of the definition of Galois category, this implies that f is an isomorphism. So X is terminal. □

Lemma 1.3.4. *Let A be a connected object. Let $\operatorname{Aut}_{\mathbf{C}}(A)$ act on $F(A)$ via $\sigma x = F(\sigma)(x)$, for any $\sigma \in \operatorname{Aut}_{\mathbf{C}}(A)$, $x \in F(A)$. Then A is Galois if and only this action is transitive (recall that an action is called* transitive *if there is exactly one orbit). In this case, the action is also free (recall that an action is called* free *if all the stabilizers are trivial) and $|\operatorname{Aut}_{\mathbf{C}}(A)| = |\operatorname{Hom}_{\mathbf{C}}(A,A)| = |F(A)|$.*

Proof. Since we know that A is connected, A is Galois if and only $A/\operatorname{Aut}_{\mathbf{C}}(A)$ is terminal. By (G5) of the definition of Galois category,

$$F(A/\operatorname{Aut}_{\mathbf{C}}(A)) \cong F(A)/F(\operatorname{Aut}_{\mathbf{C}}(A)) .$$

Then $A/\operatorname{Aut}_{\mathbf{C}}(A)$ is terminal if and only if $|F(A)/F(\operatorname{Aut}_{\mathbf{C}}(A))| = 1$, by lemma 1.3.3. But, by example 1.1.3(5), $F(A)/F(\operatorname{Aut}_{\mathbf{C}}(A))$ is the set of orbits of $F(A)$ under the action of $F(\operatorname{Aut}_{\mathbf{C}}(A))$. So $A/\operatorname{Aut}_{\mathbf{C}}(A)$ is terminal if and only if the action of $F(\operatorname{Aut}_{\mathbf{C}}(A))$ on $F(A)$ has exactly one orbit, i.e. if and only if this action is transitive. From the definition of the action of $\operatorname{Aut}_{\mathbf{C}}(A)$ on $F(A)$, it is clear that it is transitive if and only if the action of $F(\operatorname{Aut}_{\mathbf{C}}(A))$ on $F(A)$ is transitive. This allows us to conclude that A is Galois if and only if the action of $\operatorname{Aut}_{\mathbf{C}}(A)$ on $F(A)$ is transitive.
We prove now that in this case the action of $\operatorname{Aut}_{\mathbf{C}}(A)$ on $F(A)$ is also free. By the orbit-stabilizer theorem, if the action is transitive we have

$$|F(A)| = \frac{|\operatorname{Aut}_{\mathbf{C}}(A)|}{|\operatorname{Stab}_{\operatorname{Aut}_{\mathbf{C}}(A)}(x)|} \leq |\operatorname{Aut}_{\mathbf{C}}(A)| ,$$

for any $x \in F(A)$. But we know that $|\operatorname{Aut}_{\mathbf{C}}(A)| \leq |\operatorname{Hom}_{\mathbf{C}}(A, A)| \leq |F(A)|$ (remark 1.3.2). Hence $|\operatorname{Aut}_{\mathbf{C}}(A)| = |\operatorname{Hom}_{\mathbf{C}}(A, A)| = |F(A)|$ and $|\operatorname{Stab}_{\operatorname{Aut}_{\mathbf{C}}(A)}(x)| = 1$ for any $x \in F(A)$, i.e. the action of $\operatorname{Aut}_{\mathbf{C}}(A)$ on $F(A)$ is free. □

Lemma 1.3.5. *Let X be an object of $\mathbf{C}$. Then there exists a pair $(A, a) \in \mathcal{I}$ (where $\mathcal{I}$ is defined as in lemma 1.2.31) such that A is Galois and $\psi^X_{(A,a)} : \operatorname{Hom}_{\mathbf{C}}(A, X) \to F(X)$ (defined as in lemma 1.2.30) is a bijection.*

Proof. By (G1) of the definition of Galois category, in $\mathbf{C}$ any collection of objects $(X_j)_{j \in J}$ with J finite admits a product (defined recursively), denoted by $\prod_{j \in J} X_j$ (if $X_j = Z$ for any $j \in J$, we can also use the notation Z^J). Then, since $F(X)$ is finite, we can consider the object $Y := \prod_{x \in F(X)} X = X^{F(X)}$. Applying inductively (G4) of the definition of Galois category, we get that there exists an isomorphism $\varphi : \prod_{x \in F(X)} F(X) = F(X)^{F(X)} \to F(Y)$, compatible with the projections. For any $x \in F(X)$, define $b_x = x$. Then $b := (b_x)_{x \in F(X)} \in \prod_{x \in F(X)} F(X)$ and $y := \varphi(b) \in F(Y)$. By proposition 1.2.20, we can write $Y = \coprod_{i=1}^n A_i$, where $q_1 : A_1 \to Y, \ldots, q_n : A_n \to Y$ are the connected components of Y. By (G5) of the definition of Galois category, we have that $F(Y) \cong \coprod_{i=1}^n F(A_i)$ (disjoint union, by example 1.1.3(3)) and the isomorphism is compatible with the inclusions. So there exists a unique $j \in \{1, \ldots, n\}$ such that $y \in \operatorname{Im}(F(q_j))$. Then there exists $a \in F(A_j)$ such that $y = F(q_j)(a)$. We claim that (A_j, a) has the desired properties.
For any $x \in F(X)$, let $p_x : Y \to X$ be the projection on the x-th factor. Then $F(p_x) \circ \varphi : \prod_{x \in F(X)} F(X) \to F(X)$ is the projection on the x-th factor. We have that $p_x \circ q_j \in \operatorname{Hom}_{\mathbf{C}}(A_j, X)$ and

$$\psi^X_{(A_j,a)}(p_x \circ q_j) = F(p_x \circ q_j)(a) = F(p_x)(F(q_j)(a)) =$$
$$= F(p_x)(y) = F(p_x)(\varphi(b)) = b_x = x .$$

Then $\psi^X_{(A_j,a)} : \mathrm{Hom}_{\mathbf{C}}(A_j, X) \to F(X)$ is surjective. By lemma 1.2.30, it is also injective. So it is a bijection. In particular, $|\mathrm{Hom}_{\mathbf{C}}(A_j, X)| = |F(X)|$. It remains to prove that A_j is Galois. By lemma 1.3.4, we have to prove that the action of $\mathrm{Aut}_{\mathbf{C}}(A_j)$ on $F(A_j)$ is transitive.
Let $a' \in F(A_j)$ and consider the map $\psi^X_{(A_j,a')} : \mathrm{Hom}_{\mathbf{C}}(A_j, X) \to F(X)$. This map is injective by lemma 1.2.30. Then it must be a bijection, because $|\mathrm{Hom}_{\mathbf{C}}(A_j, X)| = |F(X)|$ and the sets are finite. Then the map

$$\psi := \psi^X_{(A_j,a')} \circ \left(\psi^X_{(A_j,a)}\right)^{-1} : F(X) \to F(X)$$

is also a bijection (i.e. a permutation of the finite set $F(X)$). By the universal property of the product, there exists a morphism $\sigma : Y \to Y$ such that $p_x \circ \sigma = p_{\psi(x)}$ for any $x \in F(X)$. Analogously, there exists a morphism $\sigma' : Y \to Y$ such that $p_x \circ \sigma' = p_{\psi^{-1}(x)}$ for any $x \in F(X)$. These morphisms are inverse to each other (by uniqueness in the universal property of the product). So σ is an automorphism of Y, i.e. $\sigma \in \mathrm{Aut}_{\mathbf{C}}(Y)$. We claim that $F(\sigma)(y) = F(q_j)(a')$. Let $x \in F(X)$. From the computation above, it follows that $\left(\psi^X_{(A_j,a)}\right)^{-1}(x) = p_x \circ q_j$. Then

$$\psi(x) = \psi^X_{(A_j,a')}\left(\left(\psi^X_{(A_j,a)}\right)^{-1}(x)\right) = \psi^X_{(A_j,a')}(p_x \circ q_j) =$$
$$= F(p_x \circ q_j)(a') = F(p_x)(F(q_j)(a')) \ .$$

On the other hand, we have that

$$F(p_x)(F(\sigma)(y)) = F(p_x \circ \sigma)(y) = F\left(p_{\psi(x)}\right)(y) = F\left(p_{\psi(x)}\right)(\varphi(b)) = b_{\psi(x)} = \psi(x) \ .$$

So $(F(p_x) \circ \varphi)(\varphi^{-1}(F(q_j)(a'))) = F(p_x)(F(q_j)(a')) = F(p_x)(F(\sigma)(y)) = (F(p_x) \circ \varphi)(\varphi^{-1}(F(\sigma)(y)))$, for any $x \in F(X)$. Recall that $F(p_x) \circ \varphi$ is the projection on the x-th factor of $\prod_{x \in F(X)} F(X)$. Since an element of a product of sets is uniquely determined by its components, this implies that $\varphi^{-1}(F(\sigma)(y)) = \varphi^{-1}(F(q_j)(a'))$. Then, since φ^{-1} is an isomorphism, $F(\sigma)(y) = F(q_j)(a')$, as we wanted.
Now, by corollary 1.2.21, we have that there exists a unique $j' \in \{1, \dots, n\}$ such that $\sigma \circ q_j$ is equivalent to $q_{j'}$, i.e. $\mathrm{Im}(F(\sigma \circ q_j)) = \mathrm{Im}(F(q_{j'}))$ (remark 1.2.16). We have that $F(\sigma \circ q_j)(a) = F(\sigma)(y) = F(q_j)(a') \in \mathrm{Im}(F(\sigma \circ q_j)) \cap \mathrm{Im}(F(q_j)) = \mathrm{Im}(F(q_{j'})) \cap \mathrm{Im}(F(q_j))$. In particular, $\mathrm{Im}(F(q_{j'})) \cap \mathrm{Im}(F(q_j)) \neq \emptyset$. Since $F(Y)$ is isomorphic to the disjoint union $\coprod_{i=1}^n F(A_i)$, we have that $\mathrm{Im}(F(q_j))$ and $\mathrm{Im}(F(q_{j'}))$ would be disjoint if we had $j \neq j'$. Then we must have $j = j'$, i.e. $\sigma \circ q_j$ is equivalent to q_j. This means that there exists an isomorphism $\widetilde{\sigma} : A_j \to A_j$ (i.e. $\widetilde{\sigma} \in \mathrm{Aut}_{\mathbf{C}}(A_j)$) such that $\sigma \circ q_j = q_j \circ \widetilde{\sigma}$. Then, applying what we proved above, we have that

$$F(q_j)(F(\widetilde{\sigma})(a)) = F(\sigma)(F(q_j)(a)) = F(\sigma)(y) = F(q_j)(a') \ .$$

Since q_j is a monomorphism, $F(q_j)$ is injective (corollary 1.2.10). Then $F(\widetilde{\sigma})(a) = a'$. Hence the action of $\mathrm{Aut}_{\mathbf{C}}(A_j)$ on $F(A_j)$ is transitive. □

Definition 1.3.6. Let I be a partially ordered set. We say that a subset J of I is *cofinal* if for every $i \in I$ there exists $j \in J$ such that $i \leq j$.

Lemma 1.3.7. *If I is a directed partially ordered set and $J \subseteq I$ is cofinal, then J is also directed.*

Proof. Let $j_1, j_2 \in J \subseteq I$. Since I is directed, there exists $k \in I$ such that $k \geq j_1$ and $k \geq j_2$. Since J is cofinal, there exists $j \in J$ such that $j \geq k$. Then, by transitivity, $j \geq j_1$ and $j \geq j_2$. Hence J is directed. □

Lemma 1.3.8. *Let I be a directed partially ordered set and $J \subseteq I$ a cofinal subset.*

(1) If $(S_i)_{i \in I}, (f_{ij} : S_i \to S_j)_{i,j \in I, i \geq j}$ is a projective system of sets (respectively, of groups or of topological spaces), then $(S_i)_{i \in J}, (f_{ij} : S_i \to S_j)_{i,j \in J, i \geq j}$ is also a projective system of sets (respectively, of groups or of topological spaces) and there is a bijection (respectively, a group isomorphism or a homeomorphism) between $\varprojlim_{i \in I} S_i$ and $\varprojlim_{j \in J} S_j$.

(2) If $(S_i)_{i \in I}, (f_{ij} : S_i \to S_j)_{i,j \in I, i \leq j}$ is an injective system of sets, then $(S_i)_{i \in J}$, $(f_{ij} : S_i \to S_j)_{i,j \in J, i \leq j}$ is also an injective system of sets and there is a bijection between $\varinjlim_{i \in I} S_i$ and $\varinjlim_{j \in J} S_j$.

(3) If $(S_i)_{i \in I}, (f_{ij} : S_i \to S_j)_{i,j \in I, i \geq j}$ is a projective system in $\mathbf{C}$, then $(S_i)_{i \in J}, (f_{ij} : S_i \to S_j)_{i,j \in J, i \geq j}$ is also a projective system in $\mathbf{C}$ and $\varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(S_i, -)$ and $\varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(S_j, -)$ are isomorphic as functors.

Proof. Notice that it makes sense to consider injective and projective limits indexed by J, because J is directed by lemma 1.3.7. It is obvious from the definitions of projective and injective systems that restricting the index set from I to J does not affect the fact of being a projective or an injective system. So we have to prove only the last part of each statement.

(1) For any $k \in I$, denote by $f_k : \varprojlim_{i \in I} S_i \to S_k$ the k-th projection. Analogously, for any $k \in J$ denote by $g_k : \varprojlim_{j \in J} S_j \to S_k$ the k-th projection. Consider the collection of maps (respectively, group homomorphisms or continuous maps) $(f_j : \varprojlim_{i \in I} S_i \to S_j)_{j \in J}$. Let $j_1, j_2 \in J$ such that $j_1 \geq j_2$. By definition of projective limit, for any $x = (x_i)_{i \in I} \in \varprojlim_{i \in I}$ we have that $(f_{j_1 j_2} \circ f_{j_1})(x) = f_{j_1 j_2}(x_{j_1}) = x_{j_2} = f_{j_2}(x)$. So $f_{j_1 j_2} \circ f_{j_1} = f_{j_2}$. Then we can apply the universal property of the projective limit to get the existence of a map (respectively, a group homomorphism or a continuous map) $\varphi : \varprojlim_{i \in I} S_i \to \varprojlim_{j \in J} S_j$ such that $f_j = g_j \circ \varphi$ for any $j \in J$.
We want now to define an inverse of φ. Let $i \in I$. Since J is cofinal, there exists $k \in J$ such that $k \geq i$. Define $h_i = f_{ki} \circ g_k : \varprojlim_{j \in J} S_j \to S_i$. Let us prove that h_i does not depend on the choice of k. Assume that $k_1, k_2 \in J$ are such that $k_1 \geq i$ and $k_2 \geq i$. Since J is directed, there exists $k \in J$ such that $k \geq k_1$ and $k \geq k_2$. By definition of projective system, we have that $f_{k_1 i} \circ f_{k k_1} = f_{ki} = f_{k_2 i} \circ f_{k k_2}$. Moreover, by definition of projective limit we have that, for any $x = (x_j)_{j \in J} \in \varprojlim_{j \in J} S_j$, $g_{k_1}(x) = f_{k k_1}(g_k(x))$ and $g_{k_2}(x) = f_{k k_2}(g_k(x))$. So $g_{k_1} = f_{k k_1} \circ g_k$ and $g_{k_2} = f_{k k_2} \circ g_k$. Then

$$f_{k_1 i} \circ g_{k_1} = f_{k_1 i} \circ f_{k k_1} \circ g_k = f_{ki} \circ g_k = f_{k_2 i} \circ f_{k k_2} \circ g_k = f_{k_2 i} \circ g_{k_2} \ .$$

This shows that h_i is well defined. Then we can consider the collection of maps (respectively, group homomorphism or continuous maps) $(h_i : \varprojlim_{j\in J} S_j \to S_i)_{i\in I}$. Let $i_1, i_2 \in I$ such that $i_1 \geq i_2$. Let $k \in J$ be such that $k \geq i_1$. Then, by transitivity, we have also that $k \geq i_2$. So, using the fact that $f_{ki_2} = f_{i_1 i_2} \circ f_{ki_1}$ (definition of projective system), we get

$$h_{i_2} = f_{ki_2} \circ g_k = f_{i_1 i_2} \circ f_{ki_1} \circ g_k = f_{i_1 i_2} \circ h_{i_1} .$$

Then we can apply the universal property of the projective limit to get the existence of a map (respectively, a group homomorphism or a continuos map) $\psi : \varprojlim_{j\in J} S_j \to \varprojlim_{i\in I} S_i$ such that $h_i = f_i \circ \psi$ for any $i \in I$.
For any $k \in I$, if $a \in J$ is such that $a \geq k$, we have

$$f_k \circ (\psi \circ \varphi) = h_k \circ \varphi = f_{ak} \circ g_a \circ \varphi = f_{ak} \circ f_a = f_k = f_k \circ \mathrm{id}_{\varprojlim_{i\in I} S_i}$$

(the fact that $f_{ak} \circ f_a = f_k$ can be proved as above). By uniqueness in the universal property of the projective limit, this implies that $\psi \circ \varphi = \mathrm{id}_{\varprojlim_{i\in I} S_i}$.
On the other hand, for any $k \in J$ we have

$$g_k \circ (\varphi \circ \psi) = f_k \circ \psi = h_k = f_{kk} \circ g_k = \mathrm{id}_{S_k} \circ g_k = g_k = g_k \circ \mathrm{id}_{\varprojlim_{j\in J} S_j}$$

(since $k \in J$ and $k \geq k$, we have that $h_k = f_{kk} \circ g_k$, moreover $f_{kk} = \mathrm{id}_{S_k}$ by definition of projective system). By uniqueness in the universal property of the projective limit, this implies that $\varphi \circ \psi = \mathrm{id}_{\varprojlim_{j\in J} S_j}$. Hence φ and ψ are inverse to each other, which proves the claim.

(2) Denote by $\sim_I$ and $\sim_J$ the equivalence relations defined respectively on $\coprod_{i\in I} S_i$ and $\coprod_{j\in J} S_j$, as in lemma 1.2.2. For any $k \in I$, define $f_k : S_k \to \varinjlim_{i\in I} S_i$, $x \mapsto [x]_{\sim_I}$. Analogously, for any $k \in J$, define $g_k : S_k \to \varinjlim_{j\in J} S_j$, $x \mapsto [x]_{\sim_J}$. Consider the collection of maps $(f_j : S_j \to \varinjlim_{i\in I} S_i)_{j\in J}$. Let $j_1, j_2 \in J$ such that $j_1 \leq j_2$. For any $x \in S_{j_1}$, we have that $f_{j_2}(f_{j_1 j_2}(x)) = [f_{j_1 j_2}(x)]_{\sim_I} = [x]_{\sim_I} = f_{j_1}(x)$ (applying the definition of $\sim_I$). So $f_{j_2} \circ f_{j_1 j_2} = f_{j_1}$, which allows us to apply to universal property of the injective limit. So there exists a map $\varphi : \varinjlim_{j\in J} S_j \to \varinjlim_{i\in I} S_i$ such that $f_j = \varphi \circ g_j$ for any $j \in J$.
We want now to define an inverse of φ. Let $i \in I$. Since J is cofinal, there exists $k \in J$ such that $k \geq i$. Define $h_i = g_k \circ f_{ik} : S_i \to \varinjlim_{j\in J} S_j$. Let us prove that h_i does not depend on the choice of k. Assume that $k_1, k_2 \in J$ are such that $k_1 \geq i$ and $k_2 \geq i$. Since J is directed, there exists $k \in J$ such that $k \geq k_1$ and $k \geq k_2$. By definition of injective system, we have that $f_{k_1 k} \circ f_{ik_1} = f_{ik} = f_{k_2 k} \circ f_{ik_2}$. Moreover, by definition of injective limit we have that, for any $x \in S_{k_1}$, $g_{k_1}(x) = [x]_{\sim_J} = [f_{k_1 k}(x)]_{\sim_J} = g_k(f_{k_1 k}(x))$. So $g_{k_1} = g_k \circ f_{k_1 k}$. Analogously, $g_{k_2} = g_k \circ f_{k_2 k}$. Then

$$g_{k_1} \circ f_{ik_1} = g_k \circ f_{k_1 k} \circ f_{ik_1} = g_k \circ f_{ik} = g_k \circ f_{k_2 k} \circ f_{ik_2} = g_{k_2} \circ f_{ik_2} .$$

This shows that h_i is well defined. Then we can consider the collection of maps $(h_i : \varprojlim_{j\in J} S_j \to S_i)_{i\in I}$. Let $i_1, i_2 \in I$ such that $i_1 \leq i_2$. Let $k \in J$ be such that $k \geq i_2$. Then, by transitivity, we have also that $k \geq i_1$. So, using the fact that $f_{i_1 k} = f_{i_2 k} \circ f_{i_1 i_2}$ (definition of injective system), we get

$$h_{i_1} = g_k \circ f_{i_1 k} = g_k \circ f_{i_2 k} \circ f_{i_1 i_2} = h_{i_2} \circ f_{i_1 i_2} \ .$$

Then we can apply the universal property of the injective limit to get the existence of a map $\psi : \varprojlim_{i \in I} S_i \to \varprojlim_{j \in J} S_j$ such that $h_i = \psi \circ f_i$ for any $i \in I$. For any $k \in J$ we have

$$(\psi \circ \varphi) \circ g_k = \psi \circ f_k = h_k = g_k \circ f_{kk} = g_k \circ \mathrm{id}_{S_k} = \mathrm{id}_{\varprojlim_{j \in J} S_j} \circ g_k$$

(since $k \in J$ and $k \geq k$, we have that $h_k = g_k \circ f_{kk}$, moreover $f_{kk} = \mathrm{id}_{S_k}$ by definition of injective system). By uniqueness in the universal property of the injective limit, this implies that $\psi \circ \varphi = \mathrm{id}_{\varprojlim_{j \in J} S_j}$. On the other hand, for any $k \in I$, if $a \in J$ is such that $a \geq k$, we have

$$(\varphi \circ \psi) \circ f_k = \varphi \circ h_k = \varphi \circ g_a \circ f_{ka} = f_a \circ f_{ka} = f_k = \mathrm{id}_{\varprojlim_{i \in I} S_i} \circ f_k$$

(the fact that $f_a \circ f_{ka} = f_k$ can be proved as above). By uniqueness in the universal property of the injective limit, this implies that $\varphi \circ \psi = \mathrm{id}_{\varprojlim_{i \in I} S_i}$. Hence φ and ψ are inverse to each other, which proves the claim.

(3) By point (2), for any object X of $\mathbf{C}$ we have a bijection

$$\varphi^X : \varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(S_j, X) \to \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(S_i, X) \ .$$

It remains to prove that these bijections are compatible with morphisms. Let X, Y be objects of $\mathbf{C}$ and $h : X \to Y$ a morphism. We have to prove that the following diagram is commutative.

$$\begin{array}{ccc}
\varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(S_j, X) & \xrightarrow{\varphi^X} & \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(S_i, X) \\
\Big\downarrow {\scriptstyle \varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(S_j, h)} & & \Big\downarrow {\scriptstyle \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h)} \\
\varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(S_j, Y) & \xrightarrow{\varphi^Y} & \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(S_i, Y)
\end{array}$$

By uniqueness in the universal property of the injective limit, it is enough to show that

$$\varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h) \circ \varphi^X \circ g_k^X = \varphi^Y \circ \varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(S_j, h) \circ g_k^X$$

for any $k \in J$, where $g_k^X : \mathrm{Hom}_C(S_k, X) \to \varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(S_j, X)$ is defined as in point (2). Let $k \in J$. We define also f_k^X, f_k^Y and g_k^Y as in point (2). By definition of φ^X and φ^Y, we have that $\varphi^X \circ g_k^X = f_k^X$ and $\varphi^Y \circ g_k^Y = f_k^Y$. Let $\vartheta \in \mathrm{Hom}_{\mathbf{C}}(S_k, X)$. By definition of the functor $\varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(S_i, -)$ (lemma 1.2.6), we have that

$$\left(\varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(S_i, h) \circ f_k^X \right) (\vartheta) = [h \circ \vartheta]_{\sim_I} = f_k^Y (h \circ \vartheta) \ .$$

Analogously,

$$\left(\varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(S_j,h)\circ g_k^X\right)(\vartheta)=[h\circ\vartheta]_{\sim_J}=g_k^Y(h\circ\vartheta)\ .$$

Then

$$\left(\varphi^Y\circ\varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(S_j,h)\circ g_k^X\right)(\vartheta)=(\varphi^Y\circ g_k^Y)(h\circ\vartheta)=$$
$$=f_k^Y(h\circ\vartheta)=\left(\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i,h)\circ f_k^X\right)(\vartheta)=$$
$$=\left(\varinjlim_{i\in I} \mathrm{Hom}_{\mathbf{C}}(S_i,h)\circ\varphi^X\circ g_k^X\right)(\vartheta)\ .$$

This ends the proof.

□

Lemma 1.3.9. *Let X, Y be objects of $\mathbf{C}$ with Y connected and $f : X \to Y$ a morphism. If X is not initial, then f is an epimorphism and $F(f)$ is surjective.*

Proof. By (G3) of the definition of Galois category, we can write $f = u' \circ u''$, where $u'' : X \to Z$ is an epimorphism and $u' : Z \to Y$ is a monomorphism. Since Y is connected, we have that either Z is initial or u' is an isomorphism. Since X is not initial, $F(X) \neq \emptyset$ (lemma 1.2.17). Then $F(Z)$ cannot be empty, because we have the map $F(u'') : F(X) \to F(Z)$. So Z is not initial (by (G5) of the definition of Galois category) and this implies that u' is an isomorphism. Since any isomorphism is an epimorphism, u' is an epimorphism. Then f is an epimorphism because it is the composition of two epimorphisms. The fact that $F(f)$ is surjective follows immediately from (G5) of the definition of Galois category. □

Lemma 1.3.10. *Let I be defined as in lemma 1.2.31 and consider*

$$J := \{[(A,a)]_\sim \in I \mid A\ \textit{Galois}\} \subseteq I\ .$$

Then J is cofinal. In particular, since I is directed, J is also directed.

Proof. Recalling the definition of I, it is enough to show that for any $(B,b) \in \mathcal{I}$ there exists $(A,a) \in \mathcal{I}$ such that A is Galois and $(A,a) \geq (B,b)$. Let $(B,b) \in \mathcal{I}$, i.e. B is a connected object and $b \in F(B)$. By lemma 1.3.5, there exists a pair $(A,a') \in \mathcal{I}$ such that A is Galois and $\psi^B_{(A,a')} : \mathrm{Hom}_{\mathbf{C}}(A,B) \to F(B)$ is bijective. Since B is connected, B is not initial (remark 1.2.13(1)). Then $F(B) \neq \emptyset$, by lemma 1.2.17. Since $\psi^B_{(A,a')}$ is bijective, this implies that $\mathrm{Hom}_{\mathbf{C}}(A,B) \neq \emptyset$, i.e. there exists a morphism $f : A \to B$. Since A is connected, A is not initial (remark 1.2.13(1)). Then we can apply lemma 1.3.9 to deduce that $F(f)$ is surjective. Then there exists $a \in A$ such that $F(f)(a) = b$. Hence $(A,a) \geq (B,b)$ and $(A,a) \in \mathcal{I}$ has the desired properties. □

Corollary 1.3.11. *F is isomorphic to the functor $\varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(A_j, -)$, where J is defined as in lemma 1.3.10 and the projective system is given as in lemma 1.2.33, restricting the index set to J.*

Proof. It follows immediately from the lemmas 1.3.10 and 1.3.8(3), together with the proposition 1.2.35. □

Remark 1.3.12. Let J be defined as in lemma 1.3.10 and let $j \in J$. Then there exists $(A, a) \in \mathcal{I}$ such that A is Galois and $j = [(A, a)]_{\sim}$. If $(B, b) \in \mathcal{I}$ is such that $[(B, b)]_{\sim} = j$, then we have that B is isomorphic to A and so B is also Galois (remark 1.3.2(2)).

Lemma 1.3.13. *Let A, B be objects of $\mathbf{C}$, with A Galois and B connected. If $\mathrm{Hom}_{\mathbf{C}}(A, B) \neq \emptyset$, then the action of $\mathrm{Aut}_{\mathbf{C}}(A)$ on $\mathrm{Hom}_{\mathbf{C}}(A, B)$ defined by $\sigma.f = f \circ \sigma^{-1}$, for any $\sigma \in \mathrm{Aut}_{\mathbf{C}}(B)$, $f \in \mathrm{Hom}_{\mathbf{C}}(A, B)$ (it is immediate to verify that this indeed an action), is transitive.*

Proof. Since A is Galois, A is connected. In particular, A is not initial (remark 1.2.13(1)). Then $F(A) \neq \emptyset$ (lemma 1.2.17), i.e. there exists $a \in F(A)$. Let $f, f' \in \mathrm{Hom}_{\mathbf{C}}(A, B)$. By lemma 1.3.9, $F(f') : F(A) \to F(B)$ is surjective. So there exists $a' \in F(A)$ such that $F(f')(a') = F(f)(a)$. Since A is Galois, $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on $F(A)$ (lemma 1.3.4). Then there exists $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$ such that $a' = F(\sigma)(a)$. Then we have

$$\psi^B_{(A,a)}(f) = F(f)(a) = F(f')(a') = F(f')(F(\sigma)(a)) = F(f' \circ \sigma)(a) = \psi^B_{(A,a)}(f' \circ \sigma) \,.$$

But $\psi^B_{(A,a)}$ is injective.Then $f = f' \circ \sigma$, which implies that $f' = f \circ \sigma^{-1} = \sigma.f$. Hence the action of $\mathrm{Aut}_{\mathbf{C}}(A)$ is transitive. □

We are now ready to define a projective system of groups whose projective limit will act on a natural way on $F(X)$, for any object X.

Proposition 1.3.14. *Let J be defined as in lemma 1.3.10. For any $j \in J \subseteq I$, choose $(A_j, a_j) \in \mathcal{I}$ as in lemma 1.2.33 (then A_j is Galois by remark 1.3.12). For any $j_1, j_2 \in J$ such that $j_1 \geq j_2$, choose $f_{j_1 j_2} : A_{j_1} \to A_{j_2}$ as in lemma 1.2.33. Let $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_{j_1})$ and consider the following diagram.*

$$\begin{array}{ccc} A_{j_1} & \xrightarrow{f_{j_1 j_2}} & A_{j_2} \\ \downarrow \sigma & & \downarrow ? \\ A_{j_1} & \xrightarrow{f_{j_1 j_2}} & A_{j_2} \end{array}$$

Then:

(1) there exists a unique $\tau_{\sigma j_1 j_2} \in \mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ such that $\tau_{\sigma j_1 j_2} \circ f_{j_1 j_2} = f_{j_1 j_2} \circ \sigma$;

(2) the map $\rho_{j_1 j_2} : \mathrm{Aut}_{\mathbf{C}}(A_{j_1}) \to \mathrm{Aut}_{\mathbf{C}}(A_{j_2})$, $\sigma \mapsto \tau_{\sigma j_1 j_2}$ is a surjective group homomorphism;

(3) $(\mathrm{Aut}_{\mathbf{C}}(A_j))_{j \in J}, (\rho_{j_1 j_2} : \mathrm{Aut}_{\mathbf{C}}(A_{j_1}) \to \mathrm{Aut}_{\mathbf{C}}(A_{j_2}))_{j_1, j_2 \in J, j_1 \geq j_2}$ is a projective system of groups.

Proof. (1) Consider $a_{j_2} \in F(A_{j_2})$ and $F(f_{j_1j_2} \circ \sigma)(a_{j_1}) \in F(A_{j_2})$. Since A_{j_2} is Galois, $\mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ acts freely and transitively on $F(A_{j_2})$, by lemma 1.3.4. Then there exists a unique $\tau_{\sigma j_1 j_2} \in \mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ such that $F(\tau_{\sigma j_1 j_2})(a_{j_2}) = F(f_{j_1j_2} \circ \sigma)(a_{j_1})$. By the choice of $f_{j_1j_2}$, we have that $a_{j_2} = F(f_{j_1j_2})(a_{j_1})$. Then we have

$$\psi^{A_{j_2}}_{(A_{j_1},a_{j_1})}(\tau_{\sigma j_1 j_2} \circ f_{j_1j_2}) = F(\tau_{\sigma j_1 j_2} \circ f_{j_1j_2})(a_{j_1}) = F(\tau_{\sigma j_1 j_2})(a_{j_2}) = \\ = F(f_{j_1j_2} \circ \sigma)(a_{j_1}) = \psi^{A_{j_2}}_{(A_{j_1},a_{j_1})}(f_{j_1j_2} \circ \sigma) \; .$$

By lemma 1.2.30, this implies that $\tau_{\sigma j_1 j_2} \circ f_{j_1j_2} = f_{j_1j_2} \circ \sigma$.
On the other hand, if $\tau \in \mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ is such that $\tau \circ f_{j_1j_2} = f_{j_1j_2} \circ \sigma$, then we have

$$F(\tau)(a_{j_2}) = F(\tau)(F(f_{j_1j_2})(a_{j_1})) = F(\tau \circ f_{j_1j_2})(a_{j_1}) = F(f_{j_1j_2} \circ \sigma)(a_{j_1}) \; .$$

This implies that $\tau = \tau_{\sigma j_1 j_2}$ and so we have uniqueness.

(2) By point (1), $\rho_{j_1j_2}$ is a well-defined map. Let $\sigma_1, \sigma_2 \in \mathrm{Aut}_{\mathbf{C}}(A_{j_1})$. Applying the definition of $\rho_{j_1j_2}$, we get that

$$(\rho_{j_1j_2}(\sigma_1) \circ \rho_{j_1j_2}(\sigma_2)) \circ f_{j_1j_2} = \rho_{j_1j_2}(\sigma_1) \circ (\rho_{j_1j_2}(\sigma_2) \circ f_{j_1j_2}) = \\ = \rho_{j_1j_2}(\sigma_1) \circ (f_{j_1j_2} \circ \sigma_2) = (\rho_{j_1j_2}(\sigma_1) \circ f_{j_1j_2}) \circ \sigma_2 = \\ = (f_{j_1j_2} \circ \sigma_1) \circ \sigma_2 = f_{j_1j_2} \circ (\sigma_1 \circ \sigma_2) \; .$$

By uniqueness in point (1), this implies that $\rho_{j_1j_2}(\sigma_1) \circ \rho_{j_1j_2}(\sigma_2) = \rho_{j_1j_2}(\sigma_1\sigma_2)$. So $\rho_{j_1j_2}$ is a group homomorphism.
We prove now that $\rho_{j_1j_2}$ is surjective. Let $\tau \in \mathrm{Aut}_{\mathbf{C}}(A_{j_2})$. Since $f_{j_1j_2} \in \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, A_{j_2})$, we have that $\mathrm{Hom}_{\mathbf{C}}(A_{j_1}, A_{j_2}) \neq \emptyset$. Since A_{j_1} is Galois and A_{j_2} is connected, we can apply lemma 1.3.13 and get that $\mathrm{Aut}_{\mathbf{C}}(A_{j_1})$ acts transitively on $\mathrm{Hom}_{\mathbf{C}}(A_{j_1}, A_{j_2})$. We have that $f_{j_1j_2} \in \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, A_{j_2})$ and $\tau \circ f_{j_1j_2} \in \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, A_{j_2})$. Then there exists $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_{j_1})$ such that $\tau \circ f_{j_1j_2} = \sigma.f_{j_1j_2} = f_{j_1j_2} \circ \sigma^{-1}$. Hence $\tau = \rho_{j_1j_2}(\sigma^{-1})$, which shows that $\rho_{j_1j_2}$ is surjective.

(3) Let $j \in J$. We have that $f_{jj} = \mathrm{id}_{A_j}$, by lemma 1.2.33. Then, for any $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_j)$, we have that $\sigma \circ f_{jj} = \sigma \circ \mathrm{id}_{A_j} = \sigma = \mathrm{id}_{A_j} \circ \sigma = f_{jj} \circ \sigma$. So $\sigma = \rho_{jj}(\sigma)$, by definition of ρ_{jj}. Hence $\rho_{jj} = \mathrm{id}_{\mathrm{Aut}_{\mathbf{C}}(A_j)}$.
Let j_1, j_2, j_3 be such that $j_1 \geq j_2 \geq j_3$. By lemma 1.2.33, we have that $f_{j_1j_3} = f_{j_2j_3} \circ f_{j_1j_2}$. Let $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_{j_1})$. Then, applying the definitions, we have

$$\rho_{j_2j_3}(\rho_{j_1j_2}(\sigma)) \circ f_{j_1j_3} = \rho_{j_2j_3}(\rho_{j_1j_2}(\sigma)) \circ f_{j_2j_3} \circ f_{j_1j_2} = \\ = f_{j_2j_3} \circ \rho_{j_1j_2}(\sigma) \circ f_{j_1j_2} = f_{j_2j_3} \circ f_{j_1j_2} \circ \sigma = f_{j_1j_3} \circ \sigma \; .$$

By definition of $\rho_{j_1j_3}$, this implies that $\rho_{j_2j_3}(\rho_{j_1j_2}(\sigma)) = \rho_{j_1j_3}(\sigma)$. So $\rho_{j_1j_3} = \rho_{j_2j_3} \circ \rho_{j_1j_2}$. This proves the claim.

□

From now on, in this section and in the next one, π will denote the projective limit of the projective system of groups defined in 1.3.14(3), unless otherwise specified. We have that π is a profinite group by definition.

Remark 1.3.15. (1) As in remark 1.2.34, we can notice that the projective system defined in 1.3.14 depends on the choice we made (for any $j \in J$ we chose $(A_j, a_j) \in \mathcal{I}$ such that $j = [(A_j, a_j)]_\sim$). However, this choice does not affect the projective limit, i.e. the profinite group π. Indeed, if for any $j \in J$ we choose $(B_j, b_j) \in \mathcal{I}$ such that $j = [(B_j, b_j)]_\sim$, then there exists a unique isomorphism $\varphi_j : B_j \to A_j$ such that $F(\varphi_j)(b_j) = a_j$. This isomorphism gives rise to a group isomorphism

$$\gamma_{\varphi_j} : \mathrm{Aut}_{\mathbf{C}}(A_j) \to \mathrm{Aut}_{\mathbf{C}}(B_j),\ \sigma \mapsto \varphi_j^{-1} \circ \sigma \circ \varphi_j \ .$$

Moreover, if $j_1, j_2 \in J$ are such that $j_1 \geq j_2$, then $g_{j_1 j_2} = \varphi_{j_2}^{-1} \circ f_{j_1 j_2} \circ \varphi_{j_1}$ is the unique morphism $B_{j_1} \to B_{j_2}$ such that $F(g_{j_1 j_2})(b_{j_1}) = b_{j_2}$. Let $\sigma \in \mathrm{Aut}_C(A_{j_1})$. Then, using the definition of $\rho_{j_1 j_2}$ (see proposition 1.3.14), we get

$$\begin{aligned} g_{j_1 j_2} \circ \gamma_{\varphi_{j_1}}(\sigma) &= \varphi_{j_2}^{-1} \circ f_{j_1 j_2} \circ \varphi_{j_1} \circ \varphi_{j_1}^{-1} \circ \sigma \circ \varphi_{j_1} = \\ &= \varphi_{j_2}^{-1} \circ f_{j_1 j_2} \circ \sigma \circ \varphi_{j_1} = \varphi_{j_2}^{-1} \circ \rho_{j_1 j_2}(\sigma) \circ f_{j_1 j_2} \circ \varphi_{j_1} = \\ &= \varphi_{j_2}^{-1} \circ \rho_{j_1 j_2}(\sigma) \circ \varphi_{j_2} \circ \varphi_{j_2}^{-1} \circ f_{j_1 j_2} \circ \varphi_{j_1} = \gamma_{\varphi_{j_2}}(\rho_{j_1 j_2}(\sigma)) \circ g_{j_1 j_2} \ . \end{aligned}$$

Then, if we define $\rho'_{j_1 j_2} : \mathrm{Aut}_{\mathbf{C}}(B_{j_1}) \to \mathrm{Aut}_{\mathbf{C}}(B_{j_2})$ in the same way as we defined ρ_{ij}, we have that $\gamma_{\varphi_{j_2}}(\rho_{j_1 j_2}(\sigma)) = \rho'_{j_1 j_2}\left(\gamma_{\varphi_{j_1}}(\sigma)\right)$. So the following diagram is commutative.

$$\begin{array}{ccc} \mathrm{Aut}_{\mathbf{C}}(A_{j_1}) & \xrightarrow{\gamma_{\varphi_{j_1}}} & \mathrm{Aut}_{\mathbf{C}}(B_{j_1}) \\ \rho_{j_1 j_2}\big\downarrow & & \big\downarrow \rho'_{j_1 j_2} \\ \mathrm{Aut}_{\mathbf{C}}(A_{j_2}) & \xrightarrow{\gamma_{\varphi_{j_2}}} & \mathrm{Hom}_{\mathbf{C}}(B_{j_2}) \end{array}$$

At this point, one can show that the map

$$\gamma : \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j) \to \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(B_j),\ (\sigma_j)_{j \in J} \mapsto \left(\gamma_{\varphi_j}(\sigma_j)\right)_{j \in J}$$

is a well-defined group isomorphism, with inverse

$$\gamma^{-1} : \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(B_j) \to \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j),\ (\sigma_j)_{j \in J} \mapsto \left(\gamma_{\varphi_j}^{-1}(\sigma_j)\right)_{j \in J} \ .$$

Hence $\varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j) \cong \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(B_j)$.

(2) Notice that the projective system defined in 1.3.14 depends on the functor F, because so does the index set J, in spite of the fact that being a Galois object does not depend on F (see remark 1.2.32(1)). So the group π depends on the fundamental functor: if we had another fundamental functor F' we would get another profinite group π'. The results that we will prove in the next section imply that $\pi \cong \pi'$ as profinite groups (see proposition 1.4.21 and theorem 1.4.34(d)).

Lemma 1.3.16. *For any $k \in J$, the k-th projection $p_k : \pi \to \mathrm{Aut}_{\mathbf{C}}(A_k)$ is surjective.*

Proof. Let $\tau \in \mathrm{Aut}_{\mathbf{C}}(A_k)$. For any $l \in J$, $l \geq k$ define

$$T_l := \left\{ (\sigma_j)_{j \in J} \in \prod_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j) \;\middle|\; \sigma_k = \tau, \quad \forall j \in J, j \leq l \quad \sigma_j = \rho_{lj}(\sigma_l) \right\} \subseteq$$
$$\subseteq \prod_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j)\,.$$

We consider the discrete topology on $\mathrm{Aut}_{\mathbf{C}}(A_j)$ (for any $j \in J$) and the product topology on $\prod_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$ (then π is a subspace of $\prod_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$). Denote by $q_l : \prod_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j) \to \mathrm{Aut}_{\mathbf{C}}(A_l)$ the l-th projection, which is continuous by definition of product topology. Moreover, for any $j_1, j_2 \in J$ with $j_1 \geq j_2$ define

$$\varphi_{j_1 j_2} : \prod_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j) \to \mathrm{Aut}_{\mathbf{C}}(A_{j_2}) \times \mathrm{Aut}_{\mathbf{C}}(A_{j_2}),\; (\sigma_j)_{j \in J} \mapsto (\sigma_{j_2}, \rho_{j_1 j_2}(\sigma_{j_1}))\,.$$

Then $\varphi_{j_1 j_2}$ is continuous, because it has components q_{j_2} and $\rho_{j_1 j_2} \circ q_{j_1}$, which are continuous. Define $\Delta_j := \{(\sigma, \sigma) \mid \sigma \in \mathrm{Aut}_{\mathbf{C}}(A_j)\} \subseteq \mathrm{Aut}_{\mathbf{C}}(A_j) \times \mathrm{Aut}_{\mathbf{C}}(A_j)$, for any $j \in J$. We have that Δ_j is closed in $\mathrm{Aut}_{\mathbf{C}}(A_j) \times \mathrm{Aut}_{\mathbf{C}}(A_j)$, because this product has the discrete topology. Moreover, $\{\tau\}$ is closed in $\mathrm{Aut}_{\mathbf{C}}(A_k)$. Then we have that

$$T_l = q_k^{-1}(\{\tau\}) \cap \left(\bigcap_{j \in J,\, j \leq l} \varphi_{lj}^{-1}(\Delta_j) \right)$$

is closed, because it is the intersection of closed subsets. Let $T := \bigcap_{\substack{l \in J \\ l \geq k}} T_l$. We claim that $T \subseteq \pi$. Let $\sigma = (\sigma_j)_{j \in J} \in T$ and let $j_1, j_2 \in J$ such that $j_1 \geq j_2$. Since J is directed (see lemma 1.3.10), there exists $l \in J$ such that $l \geq j_1$ and $l \geq k$. By transitivity we have also $l \geq j_2$. Since $T \subseteq T_l$, we have that $\sigma_{j_1} = \rho_{lj_1}(\sigma_l)$ and $\sigma_{j_2} = \rho_{lj_2}(\sigma_l)$. But $\rho_{lj_2} = \rho_{j_1 j_2} \circ \rho_{lj_1}$. Then $\sigma_{j_2} = \rho_{lj_2}(\sigma_l) = \rho_{j_1 j_2}(\rho_{lj_1}(\sigma_l)) = \rho_{j_1 j_2}(\sigma_{j_1})$. This shows that $\sigma \in \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j) = \pi$.

We prove now that $T \neq \emptyset$. For any $j \in J$, $\mathrm{Aut}_{\mathbf{C}}(A_j)$ is compact, because it is finite. Then, by Tichonov's theorem, the product $\prod_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$ is compact. So, in order to show that T is non-empty, it is enough to prove that $T_{l_1} \cap \cdots \cap T_{l_n} \neq \emptyset$ for any $n \in \mathbb{N}$, $l_1, \ldots, l_n \in J$ with $l_1, \ldots, l_n \geq k$. Given such $l_1, \ldots, l_n$, since J is directed, there exists $l \in J$ such that $l \geq l_i$ for any $i = 1, \ldots, n$. By transitivity, we have that $l \geq k$. We have that

$$T_l = q_k^{-1}(\{\tau\}) \cap \left(\bigcap_{j \in J,\, j \leq l} \varphi_{lj}^{-1}(\Delta_j) \right) \subseteq q_k^{-1}(\{\tau\}) \cap \left(\bigcap_{j \in J,\, j \leq l_i} \varphi_{lj}^{-1}(\Delta_j) \right) = T_{l_i}$$

for any $i = 1, \ldots, n$. Then $T_l \subseteq T_{l_1} \cap \cdots \cap T_{l_n}$. By proposition 1.3.14(2), ρ_{lk} is surjective. Then there exists $\tau' \in \mathrm{Aut}_{\mathbf{C}}(A_l)$ such that $\rho_{lk}(\tau') = \tau$. For any $j \in J$, define $\sigma_j = \mathrm{id}_{A_j}$ if $j > l$ and $\sigma_j = \rho_{lj}(\tau')$ otherwise. Then $\sigma := (\sigma_j)_{j \in J} \in \prod_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$. Moreover, $\sigma_k = \rho_{lk}(\tau') = \tau$ and the other condition that appears in the definition of T_l is automatically satisfied. So $\sigma \in T_l$. This shows that $T_l \neq \emptyset$. Since $T_l \subseteq T_{l_1} \cap \cdots \cap T_{l_n}$, we have that also $T_{l_1} \cap \cdots \cap T_{l_n} \neq \emptyset$, as we wanted. Then $T \neq \emptyset$. If $\sigma = (\sigma_j)_{j \in J} \in T$, we have that $\sigma \in \pi$ and $p_k(\sigma) = \sigma_k = \tau$. This ends the proof. □

Remark 1.3.17. It is clear from the proof of lemma 1.3.16 that this results (i.e. the fact that the projections are surjective) holds for the projective limit of any projective system of finite groups $I, (\pi_i)_{i \in I}, (f_{ij} : \pi_i \to \pi_j)_{i,j \in I, i \geq j}$ with f_{ij} surjective for any $i, j \in I$ with $i \geq j$.

1.4 The main theorem about Galois categories

Now that we have defined the profinite group π, we want to show that $\mathbf{C}$ is equivalent to the category π**-sets**. First of all, we have to define a functor $H : \mathbf{C} \to \pi\text{-}\mathbf{sets}$. To do this, we will show that π acts in a natural way on $F(X)$, for any object X of $\mathbf{C}$ and that, if $h : X \to Y$ is a morphism in $\mathbf{C}$ then $F(h) : F(X) \to F(Y)$ is a morphism of π-sets. If we fix an object X, by corollary 1.3.11 we have that $F(X) \cong \varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(A_j, X)$. Moreover, we have that $\mathrm{Aut}_C(A_j)$ acts in a natural way on $\mathrm{Hom}_{\mathbf{C}}(A_j, X)$, via $\sigma.f = f \circ \sigma^{-1}$ for any $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_j)$, $f \in \mathrm{Hom}_{\mathbf{C}}(A_j, X)$ (in lemma 1.3.13 we proved that this action is transitive when X is connected). We would like to "glue" these actions and get an action of $\pi = \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$ on $\varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(A_j, X) \cong F(X)$. To do it, we will need the following lemma.

Lemma 1.4.1. *Let I be any directed partially ordered set (here we do not refer to the notation we established in lemma 1.2.31) and consider a projective system of finite groups $(\pi_i)_{i \in I}, (\rho_{ij} : \pi_i \to \pi_j)_{i,j \in I, i \geq j}$ and an injective system of sets $(S_i)_{i \in I}, (f_{ij} : S_i \to S_j)_{i,j \in I, i \leq j}$. Assume that, for any $i \in I$, we have an action of π_i on S_i. Assume moreover that, if $i, j \in I$ are such that $i \geq j$, we have $f_{ji}(\rho_{ij}(\sigma)x) = \sigma f_{ji}(x)$ for any $\sigma \in \pi_i$, $x \in S_j$. For any $\sigma = (\sigma_i)_{i \in I} \in \varprojlim_{i \in I} \pi_i$, $X \in \varinjlim_{i \in I} S_i$, define $\sigma X = [\sigma_j x]_\sim$, if $x \in S_j$ is such that $X = [x]_\sim$. Then this is a well-defined continuous action of the profinite group $\varprojlim_{i \in I} \pi_i$ on the set $\varinjlim_{i \in I} S_i$.*

Proof. Let $\sigma = (\sigma_i)_{i \in I} \in \varprojlim_{i \in I} \pi_i$, $X \in \varinjlim_{i \in I} S_i$. We have to prove that σX is well defined. Assume that $x_1 \in S_{j_1}$, $x_2 \in S_{j_2}$ are such that $X = [x_1]_\sim = [x_2]_\sim$ ($j_1, j_2 \in I$). By definition of injective limit, this means there exists $j \in I$ such that $j \geq j_1$ and $j \geq j_2$ and $f_{j_1 j}(x_1) = f_{j_2 j}(x_2)$. Using the assumption, we get that

$$f_{j_1 j}(\rho_{j j_1}(\sigma_j) x_1) = \sigma_j f_{j_1 j}(x_1) = \sigma_j f_{j_2 j}(x_2) = f_{j_2 j}(\rho_{j j_2}(\sigma_j) x_2) .$$

By definition of projective limit, $\rho_{j j_1}(\sigma_j) = \sigma_{j_1}$ and $\rho_{j j_2}(\sigma_j) = \sigma_{j_2}$. So $f_{j_1 j}(\sigma_{j_1} x_1) = f_{j_2 j}(\sigma_{j_2} x_2)$. By definition of injective limit, this implies that $[\sigma_{j_1} x_1]_\sim = [\sigma_{j_2} x_2]_\sim$. This show that σX is well defined.
Let $X = [x]_\sim \in \varinjlim_{i \in I} S_i$, with $x \in S_j$ ($j \in I$). Since $1 = (1_i)_{i \in I}$, we have that $1X = [1_j x]_\sim = [x]_\sim$. Moreover, if $\sigma = (\sigma_i)_{i \in I}, \tau = (\tau_i)_{i \in I} \in \varprojlim_{i \in I} \pi_i$, we have that

$$(\sigma\tau)X = (\sigma_i \tau_i)_{i \in I} X = [(\sigma_j \tau_j)x]_\sim = [\sigma_j(\tau_j x)]_\sim = \sigma[\tau_j x]_\sim = \sigma(\tau X) .$$

So we have an action of $\varprojlim_{i\in I}\pi_i$ on $\varinjlim_{i\in I} S_i$. It remains to prove that this action is continuous.
Let $X = [x]_\sim \in \varinjlim_{i\in I} S_i$, with $x \in S_j$ $(j \in I)$. We have that

$$\begin{aligned}\mathrm{Stab}_{\varprojlim_{i\in I}\pi_i}(X) &= \left\{ \sigma = (\sigma_i)_{i\in I} \in \varprojlim_{i\in I}\pi_i \;\middle|\; [x]_\sim = X = \sigma X = [\sigma_j x]_\sim \right\} = \\ &= \left\{ \sigma = (\sigma_i)_{i\in I} \in \varprojlim_{i\in I}\pi_i \;\middle|\; \exists k \in I : k \geq j, \right. \\ &\qquad \left. f_{jk}(x) = f_{jk}(\sigma_j x) = f_{jk}(\rho_{kj}(\sigma_k)x) = \sigma_k f_{jk}(x) \right\} = \\ &= \bigcup_{\substack{k\in I\\ k\geq j}} \left\{ \sigma = (\sigma_i)_{i\in I} \in \varprojlim_{i\in I}\pi_i \;\middle|\; f_{jk}(x) = \sigma_k f_{jk}(x) \right\} = \bigcup_{\substack{k\in I\\ k\geq j}} p_k^{-1}\left(\mathrm{Stab}_{\pi_k}\left(f_{jk}(x)\right)\right) ,\end{aligned}$$

where $p_k : \varprojlim_{i\in I}\pi_i \to \pi_k$ is the k-th projection, for any $k \in I$. By definition of the topology on the projective limit, the projections are continuous. Since on π_k we have the discrete topology, $\mathrm{Stab}_{\pi_k}(f_{jk}(x))$ is open in π_k and so $p_k^{-1}\left(\mathrm{Stab}_{\pi_k}\left(f_{jk}(x)\right)\right)$ is open in $\varprojlim_{i\in I}\pi_i$, for any $k \in I$. Then $\mathrm{Stab}_{\varprojlim_{i\in I}\pi_i}(X)$ is open in $\varprojlim_{i\in I}\pi_i$, because it is a union of open subsets. Since this holds for any $X \in \varinjlim_{i\in I} S_i$, the action is continuous by lemma 1.1.14. □

Lemma 1.4.2. *Recall that we defined $\pi = \varprojlim_{j\in J}\mathrm{Aut}_{\mathbf{C}}(A_j)$, where the projective system is defined as in proposition 1.3.14(3). For any object X of $\mathbf{C}$, we have a continuous action of π on $\varinjlim_{j\in J}\mathrm{Hom}_{\mathbf{C}}(A_j, X)$, defined by*

$$\sigma\Phi = [\varphi \circ \sigma_k^{-1}]_\sim$$

*for any $\sigma = (\sigma_j)_{j\in J} \in \pi$ and $\Phi = [\varphi]_\sim \in \varinjlim_{j\in J}\mathrm{Hom}_{\mathbf{C}}(A_j, X)$, where $k \in J$ is such that $\varphi \in \mathrm{Hom}_{\mathbf{C}}(A_k, X)$. Since $\varinjlim_{j\in J}\mathrm{Hom}_{\mathbf{C}}(A_j, X) \cong F(X)$, this induces an action of π on $F(X)$. We denote by $H(X)$ the set $F(X)$ equipped with this action. Then $H(X)$ is an object of π-**sets** (recall that $F(X)$ is a finite set). Moreover, if X, Y are objects of $\mathbf{C}$ with a morphism $h : X \to Y$, then $F(h)$ is a morphism of π-sets. If we set $H(h) = F(h)$, then $H : \mathbf{C} \to \pi$-**sets** is a functor.*

Proof. Let X be an object of $\mathbf{C}$. For any $j \in J$, we have an action of $\mathrm{Aut}_{\mathbf{C}}(A_j)$ on $\mathrm{Hom}_{\mathbf{C}}(A_j, X)$, defined by $\sigma.f = f \circ \sigma^{-1}$, for any $\sigma \in \mathrm{Aut}_{\mathbf{C}}(S_j)$, $f \in \mathrm{Hom}_{\mathbf{C}}(A_j, X)$. We have to check that the assumptions of lemma 1.4.1 are satisfied. Let $j_1, j_2 \in J$ such that $j_1 \geq j_2$. Let $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_{j_1})$, $f \in \mathrm{Hom}_{\mathbf{C}}(A_{j_2}, X)$. Applying the definition of $\rho_{j_1 j_2}$ and the fact that it is a group homomorphism (proposition 1.3.14(2)), we get that

$$\begin{aligned} f_{j_1 j_2}^*\left(\rho_{j_1 j_2}(\sigma).f\right) &= \left(\rho_{j_1 j_2}(\sigma).f\right) \circ f_{j_1 j_2} = f \circ \left(\rho_{j_1 j_2}(\sigma)\right)^{-1} \circ f_{j_1 j_2} = \\ &= f \circ \rho_{j_1 j_2}\left(\sigma^{-1}\right) \circ f_{j_1 j_2} = f \circ f_{j_1 j_2} \circ \sigma^{-1} = f_{j_1 j_2}^*(f) \circ \sigma^{-1} = \sigma.f_{j_1 j_2}^*(f) ,\end{aligned}$$

which is precisely what we needed. Then lemma 1.4.1 gives us the desired continuous action.
Let X, Y be objects of $\mathbf{C}$ and $h : X \to Y$ a morphism. In order to show that $F(h) : F(X) \to F(Y)$ is a morphism of π-sets, we have to show that $\varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h) : \varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, X) \to \varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, Y)$ is a morphism of π-sets, because the action of π on $F(X)$ and $F(Y)$ is induced by that on $\varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, X)$ and $\varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, Y)$. Let $\sigma = (\sigma_j)_{j\in J} \in \pi$ and $\Phi = [\varphi]_\sim \in \varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, X)$, with $\varphi \in \mathrm{Hom}_{\mathbf{C}}(A_k, X)$ $(k \in J)$. Then we have

$$\begin{aligned}\varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h)(\sigma\Phi) &= \varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h)\left([\varphi \circ \sigma_k^{-1}]_\sim\right) = \\ &= [h \circ \varphi \circ \sigma_k^{-1}]_\sim = \sigma[h \circ \varphi]_\sim = \sigma \varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h)(\Phi)\ .\end{aligned}$$

Hence $\varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h)$ is a morphism of π-sets.
It remains to prove that H is a functor. This follows immediately from the fact that F is a functor. Indeed, $H(\mathrm{id}_X) = F(\mathrm{id}_X) = \mathrm{id}_{F(X)} = \mathrm{id}_{H(X)}$ for any object X of $\mathbf{C}$ and $H(h_2 \circ h_1) = F(h_2 \circ h_1) = F(h_2) \circ F(h_1) = H(h_2) \circ H(h_1)$ for any $h_1 : X \to Y$, $h_2 : Y \to Z$ morphisms in $\mathbf{C}$. □

Remark 1.4.3. If H is the functor defined in 1.4.2, we have that $\mathrm{for} \circ H = F$, where $\mathrm{for} : \pi\text{-}\mathbf{sets} \to \mathbf{sets}$ is the forgetful functor.

Now that we have the functor H, we have to prove that it is an equivalence of categories. First of all, we recall the definition of equivalence of categories and a useful characterization.

Definition 1.4.4. Let $\mathbf{C}_1$ and $\mathbf{C}_2$ be categories and $G : \mathbf{C}_1 \to \mathbf{C}_2$ a functor. We say that G is:

(1) an *equivalence of categories* if there exists a functor $G' : \mathbf{C}_2 \to \mathbf{C}_1$ such that $G' \circ G$ is isomorphic to $\mathrm{id}_{\mathbf{C}_1}$ and $G \circ G'$ is isomorphic to $\mathrm{id}_{\mathbf{C}_2}$ (in this case G' is called a *quasi-inverse* of G);

(2) *faithful* if for every two objects X, Y in $\mathbf{C}_1$ the map

$$\mathrm{Hom}_{\mathbf{C}_1}(X, Y) \to \mathrm{Hom}_{\mathbf{C}_2}(G(X), G(Y)),\ f \mapsto G(f)$$

is injective;

(3) *full* if for every two objects X, Y in $\mathbf{C}_1$ the map

$$\mathrm{Hom}_{\mathbf{C}_1}(X, Y) \to \mathrm{Hom}_{\mathbf{C}_2}(G(X), G(Y)),\ f \mapsto G(f)$$

is surjective;

(4) *fully faithful* if it is full and faithful, i.e. if for every two objects X, Y in $\mathbf{C}_1$ the map $\mathrm{Hom}_{\mathbf{C}_1}(X, Y) \to \mathrm{Hom}_{\mathbf{C}_2}(G(X), G(Y)),\ f \mapsto G(f)$ is bijective;

(5) *essentially surjective* if for every object Z of $\mathbf{C}_2$ there exists an object X of $\mathbf{C}_1$ such that $Z \cong G(X)$.

Lemma 1.4.5. *Let $\mathbf{C}_1$ and $\mathbf{C}_2$ be categories and $G : \mathbf{C}_1 \to \mathbf{C}_2$ a functor. Then G is an equivalence of categories if and only if it is fully faithful and essentially surjective.*

Proof. Assume that G is an equivalence of categories and let G' be a quasi-inverse of G. Let X, Y be objects of $\mathbf{C}_1$. Since $G' \circ G$ is isomorphic to $\mathrm{id}_{\mathbf{C}_1}$, there exist isomorphisms $\alpha_X : X \to (G' \circ G)(X)$, $\alpha_Y : Y \to (G' \circ G)(Y)$ such that for any $f \in \mathrm{Hom}_{C_1}(X, Y)$ the following diagram is commutative.

$$\begin{array}{ccc} X & \xrightarrow{\alpha_X} & (G' \circ G)(X) \\ f\downarrow & & \downarrow(G' \circ G)(f) \\ Y & \xrightarrow{\alpha_Y} & (G' \circ G)(Y) \end{array}$$

This means that $f = \alpha_Y^{-1} \circ (G' \circ G)(f) \circ \alpha_X$, for any morphism $f : X \to Y$. Assume now that $f, g : X \to Y$ are such that $G(f) = G(g)$. Then $(G' \circ G)(f) = (G' \circ G)(g)$ and so $f = \alpha_Y^{-1} \circ (G' \circ G)(f) \circ \alpha_X = \alpha_Y^{-1} \circ (G' \circ G)(g) \circ \alpha_X = g$. This shows that G is faithful. Analogously, one can show that G' is faithful. Consider now $h \in \mathrm{Hom}_{\mathbf{C}_2}(G(X), G(Y))$. We have that $\alpha_Y^{-1} \circ G'(h) \circ \alpha_X \in \mathrm{Hom}_{\mathbf{C}_1}(X, Y)$. Then

$$\alpha_Y^{-1} \circ G'(h) \circ \alpha_X = \alpha_Y^{-1} \circ (G' \circ G)(\alpha_Y^{-1} \circ G'(h) \circ \alpha_X) \circ \alpha_X \ ,$$

which implies $G'(h) = (G' \circ G)(\alpha_Y^{-1} \circ G'(h) \circ \alpha_X) = G'(G(\alpha_Y^{-1} \circ G'(h) \circ \alpha_X))$. Since G' is faithful, we get $h = G(\alpha_Y^{-1} \circ G'(h) \circ \alpha_X)$, which shows that G is full. Finally, if Z is an object of $\mathbf{C}_2$, we have that $G(G'(Z)) = (G \circ G')(Z) \cong Z$, because $G \circ G'$ is isomorphic to $\mathrm{id}_{\mathbf{C}_2}$. Hence G is essentially surjective.

Conversely, assume that G is fully faithful and essentially surjective. Since G is essentially surjective, for any object Z of $\mathbf{C}_2$, we can choose an object X_Z in $\mathbf{C}_1$ such that $G(X_Z) \cong Z$. We choose also an isomorphism $\beta_Z : G(X_Z) \to Z$. Define $G'(Z) = X_Z$. Moreover, let Z, W be objects of $\mathbf{C}_2$ and let $h : Z \to W$ be a morphism. Consider $\beta_W^{-1} \circ h \circ \beta_Z \in \mathrm{Hom}_{\mathbf{C}_2}(G(X_Z), G(X_W))$. Since G is fully faithful, there exists a unique $f_h \in \mathrm{Hom}_{\mathbf{C}_1}(X_Z, X_W)$ such that $\beta_W^{-1} \circ h \circ \beta_Z = G(f_h)$. We define $G'(h) = f_h$.

Let us check that G' is a functor. For any object Z of $\mathbf{C}_2$, we have that $G(\mathrm{id}_{X_Z}) = \mathrm{id}_{G(X_Z)} = \beta_Z^{-1} \circ \mathrm{id}_Z \circ \beta_Z$. Then $\mathrm{id}_{X_Z} = G'(\mathrm{id}_Z)$, by definition. Let Z_1, Z_2, Z_3 be objects of $\mathbf{C}_2$, with morphisms $h_1 : Z_1 \to Z_2$ and $h_2 : Z_2 \to Z_3$. We have that

$$\begin{aligned} \beta_{Z_3}^{-1} \circ (h_2 \circ h_1) \circ \beta_{Z_1} &= \left(\beta_{Z_3}^{-1} \circ h_2 \circ \beta_{Z_2}\right) \circ \left(\beta_{Z_2}^{-1} \circ h_1 \circ \beta_{Z_1}\right) = \\ &= G(f_{h_2}) \circ G(f_{h_1}) = G(f_{h_2} \circ f_{h_1}) \ . \end{aligned}$$

This shows that $G'(h_2 \circ h_1) = f_{h_2 \circ h_1} = f_{h_2} \circ f_{h_1} = G'(h_2) \circ G'(h_1)$. So G' is a functor. We check now that G' is a quasi-inverse of G. First of all, we show that $G \circ G'$ is isomorphic to $\mathrm{id}_{\mathbf{C}_2}$. We already have the isomorphisms $\beta_Z : G(X_Z) = (G \circ G')(Z) \to Z$, for any object Z of $\mathbf{C}_2$. We have to show that these isomorphisms are compatible with each other. Let Z, W be two objects of $\mathbf{C}_2$, with a morphism $h : Z \to W$. We have to show that the following diagram is commutative.

$$\begin{array}{ccc} (G\circ G')(Z) & \xrightarrow{\beta_Z} & Z \\ {\scriptstyle (G\circ G')(h)}\downarrow & & \downarrow{\scriptstyle h} \\ (G\circ G')(W) & \xrightarrow{\beta_W} & W \end{array}$$

By definition, $(G \circ G')(h) = G(f_h) = \beta_W^{-1} \circ h \circ \beta_Z$, which is exactly what we need. On the other hand, we have to show that $G' \circ G$ is isomorphic to $\mathrm{id}_{\mathbf{C}_1}$. Let X be an object of $\mathbf{C}_1$. Then we have an isomorphism $\beta_{G(X)} : G((G' \circ G)(X)) = (G \circ G')(G(X)) \to G(X)$. Since G is fully faithful, there exists a unique morphism $\alpha_X : (G' \circ G)(X) \to X$ such that $\beta_{G(X)} = G(\alpha_X)$. Analogously, there exists a unique morphism $\alpha'_X : X \to (G' \circ G)(X)$ such that $\beta_{G(X)}^{-1} = G(\alpha'_X)$. Then

$$G(\alpha_X \circ \alpha'_X) = G(\alpha_X) \circ G(\alpha'_X) = \beta_{G(X)} \circ \beta_{G(X)}^{-1} = \mathrm{id}_{G(X)} = G(\mathrm{id}_X)$$

and

$$G(\alpha'_X \circ \alpha_X) = G(\alpha'_X) \circ G(\alpha_X) = \beta_{G(X)}^{-1} \circ \beta_{G(X)} = \mathrm{id}_{G((G' \circ G)(X))} = G\left(\mathrm{id}_{(G' \circ G)(X)}\right) .$$

Since G is faithful, this implies that $\alpha_X \circ \alpha'_X = \mathrm{id}_X$ and $\alpha'_X \circ \alpha_X = \mathrm{id}_{(G' \circ G)(X)}$. This shows that α_X is an isomorphism. Again, we have to show that the isomorphisms α_X's are compatible with each other. Let X, Y be objects of $\mathbf{C}_1$ and $f : X \to Y$ a morphism. We have to show that the following diagram is commutative.

$$\begin{array}{ccc} (G'\circ G)(X) & \xrightarrow{\alpha_X} & X \\ {\scriptstyle (G'\circ G)(f)}\downarrow & & \downarrow{\scriptstyle f} \\ (G'\circ G)(Y) & \xrightarrow{\alpha_Y} & Y \end{array}$$

By definition of G', we have that

$$G((G' \circ G)(f)) = \beta_{G(Y)}^{-1} \circ G(f) \circ \beta_{G(X)} = G(\alpha_Y)^{-1} \circ G(f) \circ G(\alpha_X) = G(\alpha_Y^{-1} \circ f \circ \alpha_X) .$$

Since G is faithful, we get $(G' \circ G)(f) = \alpha_Y^{-1} \circ f \circ \alpha_X$, which ends the proof. □

Lemma 1.4.6. *The fundamental functor F is faithful.*

Proof. Let X, Y be objects of $\mathbf{C}$ and let $f, g : X \to Y$ be morphisms such that $F(f) = F(g)$. Consider the equalizer $\mathrm{Eq}(f, g)$, with the morphism $\iota : \mathrm{Eq}(f, g) \to X$, as in the definition 1.2.23 (this equalizer exists by lemma 1.2.26). By corollary 1.2.27, we have an isomorphism $\varphi : \mathrm{Eq}(F(f), F(g)) \to F(\mathrm{Eq}(f, g))$ such that $F(\iota) \circ \varphi$ is the inclusion of $\mathrm{Eq}(F(f), F(g))$ inside $F(X)$. But $\mathrm{Eq}(F(f), F(g)) = \{x \in F(X) \mid F(f)(x) = F(g)(x)\} = F(X)$, since $F(f) = F(g)$ (see example 1.2.25 for the equalizer in **sets**). So $F(\iota) \circ \varphi$ is an isomorphism. Since φ is also an isomorphism, we must have that $F(\iota)$ is an isomorphism, which by (G6) of the definition of Galois category implies that ι is an isomorphism. Then by $f \circ \iota = g \circ \iota$ (see the definition of equalizer) we get $f = g$. □

Lemma 1.4.7. *Let $\mathbf{C}_1$, $\mathbf{C}_2$,$\mathbf{C}_3$ be categories and $G_1 : \mathbf{C}_1 \to \mathbf{C}_2$, $G_2 : \mathbf{C}_2 \to \mathbf{C}_3$ functors. If $G_2 \circ G_1 : \mathbf{C}_1 \to \mathbf{C}_3$ is faithful, then G_1 is also faithfull.*

Proof. Let X, Y be objects of $\mathbf{C}_1$ and let $f, g : X \to Y$ be morphisms such that $G_1(f) = G_1(g)$. Then $(G_2 \circ G_1)(f) = G_2(G_1(f)) = G_2(G_1(g)) = (G_2 \circ G_1)(g)$. Since $G_2 \circ G_1$ is faithful, this implies that $f = g$. Hence G_1 is faithful. □

Corollary 1.4.8. *The functor H defined in 1.4.2 is faithful.*

Proof. It follows from the lemmas 1.4.6 and 1.4.7, together with the remark 1.4.3. □

Before proving that H is essentially surjective, we need to understand the structure of the object of π-**sets**. Since π-**sets** is a Galois category (proposition 1.1.15), we know that any object is the sum of its connected components (proposition 1.2.20) and that this decomposition corresponds to the orbit decomposition (see example 1.2.22). What we do not know yet is how the connected objects, i.e. the finite sets with a transitive continuous action of π (example 1.2.14(2)), look like.

Lemma 1.4.9. *In this lemma, we do not use the notation introduced in proposition 1.3.14 and we denote by π an arbitrary profinite group. Let E be a finite set with a transitive continuous action of π.*

(1) There exists an open subgroup $\pi' \leq \pi$ such that E is isomorphic as a π-set to π/π' with the action given by left multiplication: $\sigma(\tau\pi') = (\sigma\tau)\pi'$ for any $\sigma \in \pi$, $\tau\pi' \in \pi/\pi'$.

(2) If π is the projective limit of the projective system of finite groups $I, (\pi_i)_{i\in I}$, $(\rho_{ij} : \pi_i \to \pi_j)_{i,j\in I, i\geq j}$ and $p_j : \pi = \varprojlim_{i\in I} \pi_i \to \pi_j$ is the canonical projection for any $j \in I$, then there exists $j \in J$ such that $\operatorname{Ker}(p_j) \leq \pi'$.

(3) Let $j \in I$ be such that $\operatorname{Ker}(p_j) \leq \pi'$, as in point (2). If p_j is surjective, then there exists a subgroup $\pi'_j \leq \pi_j$ such that E is isomorphic as a π-set to π_j/π'_j, with the action given by $\sigma(x\pi'_j) = (\sigma_j x)\pi'_j$, for any $\sigma = (\sigma_i)_{i\in I} \in \pi$, $x\pi'_j \in \pi_j/\pi'_j$.

Proof. (1) Since the action of π on E is transitive, E is non-empty. Fix $e \in E$ and define $\pi' = \operatorname{Stab}_\pi(e)$. Then π' is an open subgroup of π by lemma 1.1.14. By lemma 1.1.11, π' has finite index in π, so π/π' is a finite set. It is easy to check that left multiplication defines indeed a continuous action of π on π/π' (see also the proof of (G3) in 1.1.15). Consider now the map

$$\varphi : \pi/\pi' \to E,\ \tau\pi' \mapsto \tau e\ .$$

First of all, we check that φ is well defined. If $\tau_1\pi' = \tau_2\pi'$, with $\tau_1, \tau_2 \in \pi$, then we have that $\tau_2^{-1}\tau_1 \in \pi' = \operatorname{Stab}_\pi(e)$. So $e = \left(\tau_2^{-1}\tau_1\right)(e) = \tau_2^{-1}(\tau_1(e))$, which implies that $\tau_1 e = \tau_2 e$. So φ is well defined. Transitivity of the action of π on E implies that φ is surjective. Moreover, if $\tau_1\pi', \tau_2\pi' \in \pi/\pi'$ are such that $\varphi(\tau_1\pi') = \varphi(\tau_2\pi')$, then $\tau_1 e = \tau_2 e$. So $\left(\tau_2^{-1}\tau_1\right) e = e$ which implies that $\tau_2^{-1}\tau_1 \in \operatorname{Stab}_\pi(e) = \pi'$. So $\tau_1\pi' = \tau_2\pi'$. Then φ is also injective. It remains to prove that φ is a morphism of π-sets (since π-**sets** is a Galois category, a morphism of π-sets is an isomorphism if and only if it is a bijection, by (G6) of the definition of Galois category). Let $\sigma \in \pi$, $\tau\pi' \in \pi/\pi'$. Then

$$\varphi(\sigma(\tau\pi')) = \varphi((\sigma\tau)\pi') = (\sigma\tau)e = \sigma(\tau e) = \sigma\varphi(\tau\pi')\ .$$

This shows that φ is a morphism of π-sets.

(2) Since π' is a subgroup, we have that $1 = (1_i)_{i\in I} \in \pi'$. Recall that the topology on π is defined as the subspace topology of the product topology, considering on each π_i the discrete topology. Then a local base for π at 1 is given by

$$\left\{ U_{j_1\dots j_n} := \bigcap_{k=1}^{n} p_{j_k}^{-1}\left(\{1_{j_k}\}\right) = \bigcap_{k=1}^{n} \mathrm{Ker}(p_{j_k}) \;\middle|\; n \in \mathbb{N},\ j_1,\dots,j_n \in I \right\} .$$

Since π' is open and $1 \in \pi'$, there exist $n \in \mathbb{N}$, $j_1,\dots,j_n \in I$ such that $U_{j_1\dots j_n} \subseteq \pi'$. Since I is directed, there exists $j \in I$ such that $j \geq j_k$ for any $k = 1,\dots,n$. We claim that $U_j = \mathrm{Ker}(p_j) \subseteq U_{j_1\dots j_n}$. Let $\sigma = (\sigma_i)_{i\in I} \in U_j \subseteq \pi$. This means that $\sigma_j = p_j(\sigma) = 1_j$. By definition of projective system, we have that $p_{j_k}(\sigma) = \sigma_{j_k} = \rho_{jj_k}(\sigma_j) = \rho_{jj_k}(1_j) = 1_{j_k}$ for any $k = 1,\dots,n$ (we used the fact that ρ_{jj_k} is a group homomorphism). Then $\sigma \in \bigcap_{k=1}^{n} \mathrm{Ker}(p_{j_k}) = U_{j_1\dots j_k}$, which proves our claim. Then $\mathrm{Ker}(p_j) \subseteq U_{j_1\dots j_n} \subseteq \pi'$.

(3) Assume that p_j is surjective and define $\pi'_j := p_j(\pi') \leq \pi_j$. First of all, we prove that the definition we gave leads indeed to a well-defined continuous group action. Let $\sigma = (\sigma_i)_{i\in I} \in \pi = \varprojlim_{i\in I} \pi_i$ and let $x_1, x_2 \in \pi_j$ such that $x_1\pi'_j = x_2\pi'_j$, i.e. $x_2^{-1}x_1 \in \pi'_j$. Then we have that $(\sigma_j x_2)^{-1}(\sigma_j x_1) = x_2^{-1}x_1 \in \pi'_j$, i.e. $(\sigma_j x_1)\pi'_j = (\sigma_j x_2)\pi'_j$. This shows that the definition we gave is unambiguous. For any $x\pi'_j \in \pi_j/\pi'_j$, we have that $1(x\pi'_j) = (1_j x)\pi'_j = x\pi'_j$ and

$$\begin{aligned}(\sigma\tau)(x\pi'_j) = (\sigma_i\tau_i)_{i\in I}(x\pi'_j) = ((\sigma_j\tau_j)x)\pi'_j &= \\ &= (\sigma_j(\tau_j x))\pi'_j = \sigma((\tau_j x)\pi'_j) = \sigma(\tau(x\pi'_j)) ,\end{aligned}$$

for any $\sigma = (\sigma_i)_{i\in I}, \tau = (\tau_i)_{i\in I} \in \pi$. So we have a group action. For any $x\pi'_j \in \pi_j/\pi'_j$, we have that

$$\begin{aligned}\mathrm{Stab}_\pi(x\pi'_j) &= \left\{\sigma = (\sigma_i)_{i\in I} \in \pi \mid x\pi'_j = \sigma(x\pi'_j) = (\sigma_j x)\pi'_j\right\} = \\ &= \left\{\sigma = (\sigma_i)_{i\in I} \in \pi \mid x^{-1}\sigma_j x \in \pi'_j\right\} = \\ &= \left\{\sigma = (\sigma_i)_{i\in I} \in \pi \mid \sigma_j \in x\pi'_j x^{-1}\right\} = p_j^{-1}\left(x\pi'_j x^{-1}\right) .\end{aligned}$$

Since the topology on π_j is the discrete one, $x\pi'_j x^{-1}$ is open in π_j. Then $p_j^{-1}\left(x\pi'_j x^{-1}\right)$ is open in π, because p_j is continuous (definition of the topology on the projective limit). So the stabilizer is open and, since this holds for any $x\pi'_j \in \pi_j/\pi'_j$, the action is continuous by lemma 1.1.14.
Consider now the map

$$\psi : \pi/\pi' \to \pi_j/\pi'_j,\ \tau\pi' \mapsto p_j(\tau)\pi'_j .$$

If $\tau_1, \tau_2 \in \pi$ are such that $\tau_1\pi' = \tau_2\pi'$, then $\tau_2^{-1}\tau_1 \in \pi'$. So

$$p_j(\tau_2)^{-1}p_j(\tau_1) = p_j\left(\tau_2^{-1}\tau_1\right) \in p_j(\pi') = \pi'_j ,$$

which implies that $p_j(\tau_1)\pi'_j = p_j(\tau_2)\pi'_j$. This shows that ψ is well defined. Since p_j is surjective, for any $x\pi'_j \in \pi_j/\pi'_j$ there exists $\tau \in \pi$ such that $p_j(\tau) = x$ and then $\psi(\tau\pi') = x\pi'_j$. So ψ is surjective. Assume that $\tau_1\pi', \tau_2\pi' \in \pi/\pi'$ are such that $\psi(\tau_1\pi') = \psi(\tau_2\pi')$. This means that $p_j(\tau_1)\pi'_j = p_j(\tau_2)\pi'_j$, i.e. $p_j\left(\tau_2^{-1}\tau_1\right) = p_j(\tau_2)^{-1}p_j(\tau_1) \in \pi'_j = p_j(\pi')$. Then there exists $\tau \in \pi'$ such that $p_j\left(\tau_2^{-1}\tau_1\right) = p_j(\tau)$, i.e. $\tau^{-1}\tau_2^{-1}\tau_1 \in \mathrm{Ker}(p_j)$. Since $\mathrm{Ker}(p_j) \leq \pi'$, we get that $\tau^{-1}\tau_2^{-1}\tau_1 \in \pi'$, i.e. $\tau_1\pi' = \tau_2\tau\pi' = \tau_2\pi'$ (in the last equality we used the fact that $\tau \in \pi'$). So ψ is also injective. If we show that ψ is a morphism of π-sets, we get that ψ is an isomorphism of π-sets. Let $\sigma = (\sigma_i)_{i\in I} \in \pi$, $\tau\pi' \in \pi/\pi'$. We have that

$$\begin{aligned}\psi(\sigma(\tau\pi')) &= \psi((\sigma\tau)\pi') = p_j(\sigma\tau)\pi'_j = \\ &= (p_j(\sigma)p_j(\tau))\pi'_j = (\sigma_j p_j(\tau))\pi'_j = \sigma(p_j(\tau)\pi'_j) = \sigma\psi(\tau\pi')\ .\end{aligned}$$

So ψ is a morphism of π-sets. Then π/π' and π_j/π'_j are isomorphic as π-sets. Combining this result with that of point (1), we get that E is isomorphic to π_j/π'_j as a π-set.

□

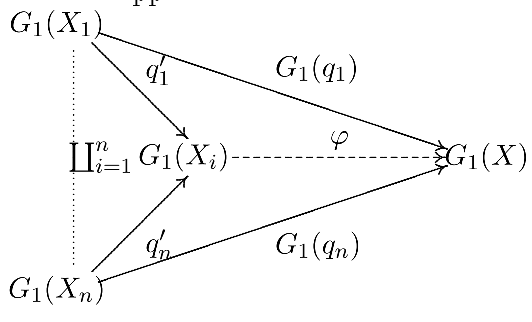
Remark 1.4.10. From the proof of lemma 1.4.9(1), it is clear that the subgroup π' is in general not unique: one can take the stabilizer of any element of E. However, these subgroups are all conjugated.

Lemma 1.4.11. *Let $\mathbf{C}_1$, $\mathbf{C}_2$,$\mathbf{C}_3$ be categories and $G_1 : \mathbf{C}_1 \to \mathbf{C}_2$, $G_2 : \mathbf{C}_2 \to \mathbf{C}_3$ functors. Assume that finite sums and quotients by finite groups of automorphisms exist in $\mathbf{C}_1$, $\mathbf{C}_2$ and $\mathbf{C}_3$. Assume moreover that G_2 has the following property: if $f : X \to Y$ is a morphism in $\mathbf{C}_2$ such that $G_2(f)$ is an isomorphism, then f is an isomorphism (a functor satisfying this property is called a* conservative *functor). If both G_2 and $G_2 \circ G_1$ commute with finite sums or with passage to the quotient by a finite group of automorphisms, then so does G_1.*

Proof. We prove the lemma in the case of finite sums. The proof in the case of quotients is analogous. Let $X_1, \ldots, X_n$ be objects of $\mathbf{C}_1$ ($n \in \mathbb{N}$). Let $X = X_1 \amalg \cdots \amalg X_n$ be the sum of $X_1, \ldots, X_n$, with morphisms $q_i : X_i \to X$ for any $i = 1, \ldots, n$. Then in $\mathbf{C}_2$ we have morphisms $G_1(q_i) : G_1(X_i) \to G_1(X)$, for any $i = 1, \ldots, n$, which lead to a unique morphism

$$\varphi : G_1(X_1) \amalg \cdots \amalg G_1(X_n) \to G_1(X)$$

such that $\varphi \circ q'_i = G_1(q_i)$ for any $i = 1, \ldots, n$, where $q'_i : G_1(X_i) \to G_1(X_1) \amalg \cdots \amalg G_1(X_n)$ is the morphism that appears in the definition of sum.



Applying G_2, we get a morphism $G_2(\varphi) : G_2(G_1(X_1) \amalg \cdots \amalg G_1(X_n)) \to (G_2 \circ G_1)(X)$ in $\mathbf{C}_3$. On the other hand, since G_2 commutes with finite sums, we have an isomorphism

$$\psi : (G_2 \circ G_1)(X_1) \amalg \cdots \amalg (G_2 \circ G_1)(X_n) \to G_2(G_1(X_1) \amalg \cdots \amalg G_1(X_n))$$

in $\mathbf{C}_3$ such that $\psi \circ q_i'' = G_2(q_i')$ for any $i = 1, \ldots, n$, where $q_i'' : (G_2 \circ G_1)(X_i) \to (G_2 \circ G_1)(X_1) \amalg \cdots \amalg (G_2 \circ G_1)(X_n)$ is the morphism that appears in the definition of sum. We have that $G_2(\varphi) \circ \psi : (G_2 \circ G_1)(X_1) \amalg \cdots \amalg (G_2 \circ G_1)(X_n) \to (G_2 \circ G_1)(X)$ satisfies $(G_2(\varphi) \circ \psi) \circ q_i'' = G_2(\varphi) \circ G_2(q_i') = G_2(\varphi \circ q_i') = (G_2 \circ G_1)(q_i)$ for any $i = 1, \ldots, n$ and, by uniqueness follows from the universal property of the sum, it is the only morphism with this property. Then $G_2(\varphi) \circ \psi$ must be an isomorphism, because $G_2 \circ G_1$ commutes with finite sums. So $G_2(\varphi) = (G_2(\varphi) \circ \psi) \circ \psi^{-1}$ is an isomorphism. By the assumption on G_2, φ is also an isomorphism, i.e. $G_1(X_1) \amalg \cdots \amalg G_1(X_n) \cong G_1(X)$. Hence G_1 commutes with finite sums. □

Corollary 1.4.12. *The functor H commutes with finite sums and with passage to the quotient by a finite group of automorphisms.*

Proof. It follows from (G5) of the definition of Galois category, together with lemma 1.4.11 and remark 1.4.3. Notice that we can apply the lemma because **π-sets** is also a Galois category and so the forgetful functor for : $\mathbf{C} \to$ **π-sets** satisfies the assumption ((G5) and (G6) of the definition of Galois category). □

Lemma 1.4.13. *Let $k \in J$. Then A_k is a Galois object of $\mathbf{C}$ (remark 1.3.12). Let G be a subgroup of $\mathrm{Aut}_{\mathbf{C}}(A_k)$ (notice that G is necessarily finite because $\mathrm{Aut}_C(A_k)$ is finite, see remark 1.3.2(1)). Consider the quotient A_k/G, which exists in $\mathbf{C}$ by (G2) of the definition of Galois category. We have that $H(A_k/G) \cong \mathrm{Aut}_C(A_k)/G$, with the action of π given by $\sigma(fG) = (\sigma_k f)G$ for any $\sigma = (\sigma_j)_{j \in J} \in \pi = \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$, $fG \in \mathrm{Aut}_{\mathbf{C}}(A_k)/G$.*

Proof. Notice that the definition we gave leads indeed to a well-defined continuous group action (this can be proved as in the proof of lemma 1.4.9).
First of all, we prove that $H(A_k) \cong \mathrm{Aut}_{\mathbf{C}}(A_k)$, with the action of π given by $\sigma f = \sigma_k f$ for any $\sigma = (\sigma_j)_{j \in J} \in \pi = \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$, $f \in \mathrm{Aut}_{\mathbf{C}}(A_k)$ (this can also be seen as the case $G = 1$). Consider the map $\psi^{A_k}_{(A_k,a_k)} : \mathrm{Aut}_{\mathbf{C}}(A_k) \to F(A_k)$. By lemma 1.2.30, this map is injective. But $|\mathrm{Aut}_{\mathbf{C}}(A_k)| = |F(A_k)|$ (lemma 1.3.4) and the sets are finite. So $\psi^{A_k}_{(A_k,a_k)}$ must be bijective. Consider the map $\iota : \mathrm{Aut}_{\mathbf{C}}(A_k) \to \mathrm{Aut}_{\mathbf{C}}(A_k)$, $f \mapsto f^{-1}$. It is clearly a bijection (with $\iota^{-1} = \iota$) and so $\psi^{A_k}_{(A_k,a_k)} \circ \iota : \mathrm{Aut}_{\mathbf{C}}(A_k) \to F(A_k)$ is a bijection. Recall that $H(A_k)$ was defined as the set $F(A_k)$ with the action given in lemma 1.4.2. Then it is enough to show that $\psi^{A_k}_{(A_k,a_k)} \circ \iota$ is a morphism of π-sets (recall that a morphism of π-sets is an isomorphism if and only if it is bijective, by (G6) of the definition of Galois category). Since the action of π on $F(A_k)$ was induced by that on $\varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(A_j, A_k)$, this is equivalent to proving that

$$\varphi := \left(\psi'_{A_k}\right)^{-1} \circ \psi^{A_k}_{(A_k,a_k)} \circ \iota$$

is a morphism of π-sets, where $\psi'_{A_k} : \varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(A_j, A_k) \to F(A_k)$ is the bijection defined as in the proof of proposition 1.2.35, but considering J as index set instead of I (it is still a bijection, because it is the composition of $\psi_{A_k} : \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, A_k) \to F(A_k)$ with the bijection $\varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(A_j, A_k) \to \varinjlim_{i \in I} \mathrm{Hom}_{\mathbf{C}}(A_i, A_k)$ defined as in lemma 1.3.8). This means that $\psi'_{A_k}([f]_\sim) = \psi^{A_j}_{(A_j, a_j)}(f)$, for any $f \in \mathrm{Hom}_{\mathbf{C}}(A_j, A_k)$. Then

$$\varphi(f) = \left(\left(\psi'_{A_k}\right)^{-1} \circ \psi^{A_k}_{(A_k, a_k)} \right) \left(f^{-1}\right) = [f^{-1}]_\sim \in \varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(A_j, A_k) \ ,$$

for any $f \in \mathrm{Aut}_{\mathbf{C}}(A_k)$. Let $\sigma = (\sigma_j)_{j \in J} \in \pi$, $f \in \mathrm{Aut}_{\mathbf{C}}(A_k)$. Then we have

$$\varphi(\sigma f) = \varphi(\sigma_k f) = [(\sigma_k f)^{-1}]_\sim = [f^{-1} \sigma_k^{-1}]_\sim = \sigma [f^{-1}]_\sim = \sigma \varphi(f)$$

(see the definition of the action in 1.4.2). Hence φ is a morphism of π-sets, as we wanted.
We consider now the general case. We have that $H(A_k/G) \cong H(A_k)/H(G)$ (quotient in π-**sets**), by corollary 1.4.12. The isomorphism of π-sets $\psi^{A_k}_{(A_k, a_k)} \circ \iota : \mathrm{Aut}_{\mathbf{C}}(A_k) \to H(A_k)$ induces an isomorphism of groups

$$\begin{aligned} \gamma : \mathrm{Aut}_{\pi\text{-}\mathbf{sets}}(H(A_k)) &\to \mathrm{Aut}_{\pi\text{-}\mathbf{sets}}(\mathrm{Aut}_{\mathbf{C}}(A_k)), \\ \alpha &\mapsto \left(\psi^{A_k}_{(A_k, a_k)} \circ \iota \right)^{-1} \circ \alpha \circ \left(\psi^{A_k}_{(A_k, a_k)} \circ \iota \right) \ , \end{aligned}$$

which sends $H(G)$ to

$$\gamma(H(G)) = \left\{ \left(\psi^{A_k}_{(A_k, a_k)} \circ \iota \right)^{-1} \circ H(g) \circ \left(\psi^{A_k}_{(A_k, a_k)} \circ \iota \right) \,\middle|\, g \in G \right\} \ .$$

We have that $H(A_k)/H(G)$ is the set of orbits of $H(A_k)$ under the action of $H(G)$ and $\mathrm{Aut}_{\mathbf{C}}(A_k)/\gamma(H(G))$ is the set of orbits of $\mathrm{Aut}_{\mathbf{C}}(A_k)$ under the action of $\gamma(H(G))$, with the induced action (see the proof of proposition 1.1.15). It is easy to check the map

$$\mathrm{Aut}_{\mathbf{C}}(A_k)/\gamma(H(G)) \to H(A_k)/H(G), \ \gamma(H(G)) f \mapsto H(G) \left(\psi^{A_k}_{(A_k, a_k)} \circ \iota \right)(f)$$

is a well-defined isomorphism of π-sets. So

$$H(A_k/G) \cong H(A_k)/H(G) \cong \mathrm{Aut}_{\mathbf{C}}(A_k)/\gamma(H(G)) \ .$$

Then it is enough to prove that the set of orbits $\mathrm{Aut}_{\mathbf{C}}(A_k)/\gamma(H(G))$ coincides with the quotient set $\mathrm{Aut}_{\mathbf{C}}(A_k)/G$ (in that case, it is clear that the two actions coincide, because they are both induced by the action on $\mathrm{Aut}_{\mathbf{C}}(A_k)$). Let $f_1, f_2 \in \mathrm{Aut}_{\mathbf{C}}(A_k)$ and assume that f_1 and f_2 are in the same orbit under the action of $\gamma(H(G))$. This means that there exists $g \in G$ such that

$$f_2 = \gamma(H(g))(f_1) = \left(\left(\psi^{A_k}_{(A_k,a_k)} \circ \iota \right)^{-1} \circ H(g) \circ \left(\psi^{A_k}_{(A_k,a_k)} \circ \iota \right) \right) (f_1) =$$
$$= \left(\iota^{-1} \circ \left(\psi^{A_k}_{(A_k,a_k)} \right)^{-1} \right) \left(H(g) \left(\psi^{A_k}_{(A_k,a_k)} (f_1^{-1}) \right) \right) =$$
$$= \left(\iota \circ \left(\psi^{A_k}_{(A_k,a_k)} \right)^{-1} \right) \left(F(g) \left(F(f_1^{-1})(a_k) \right) \right) =$$
$$= \iota \left(\left(\psi^{A_k}_{(A_k,a_k)} \right)^{-1} \left(F(g \circ f_1^{-1})(a_k) \right) \right) = \iota(g \circ f_1^{-1}) = f_1 \circ g^{-1} \, .$$

Since $g^{-1} \in G$, this implies that $f_2 \in f_1 G$ and so $f_2 G = f_1 G$. Conversely, assume that $f_2 G = f_1 G$. Then there exists $g \in G$ such that $f_2 = f_1 g = \gamma(H(g^{-1}))(f_1)$ and so f_1 and f_2 are in the same orbit under the action of $\gamma(H(G))$. This ends the proof. □

Remark 1.4.14. For the sake of convenience, the lemma 1.4.13 was stated for Galois objects of the form A_k with $k \in J$. However, it can be generalized to arbitrary Galois objects. Let A be a Galois object of $\mathbf{C}$ and let G be a subgroup of $\mathrm{Aut}_{\mathbf{C}}(A)$ (again, G is finite because $\mathrm{Aut}_{\mathbf{C}}(A)$ is finite). Fix $a \in F(A)$ (since A is connected, by remark 1.2.13 it is not initial and so $F(A) \neq \emptyset$ by lemma 1.2.17). Then $k := [(A,a)]_\sim \in J$ and, since $[(A,a)]_\sim = k = [(A_k,a_k)]_\sim$, we have that $A \sim A_k$, i.e. there exists an isomorphism $\varphi : A \to A_k$ such that $F(\varphi)(a) = a_k$. This isomorphisms induces the following isomorphism of groups: $\gamma_\varphi : \mathrm{Aut}_{\mathbf{C}}(A_k) \to \mathrm{Aut}_{\mathbf{C}}(A)$, $f \mapsto \varphi^{-1} \circ f \circ \varphi$. Then we have a bijection $\mathrm{Aut}_{\mathbf{C}}(A)/G \cong \mathrm{Aut}_{\mathbf{C}}(A_k)/\gamma_\varphi^{-1}(G)$. Since π acts on $\mathrm{Aut}_{\mathbf{C}}(A_k)/\gamma_\varphi^{-1}(G)$ as in lemma 1.4.13, we can induce an action of π on $\mathrm{Aut}_{\mathbf{C}}(A)/G$ such that this bijection becomes an isomorphism of π-sets. It is easy to verify that $A/G \cong A_k/\gamma_\varphi^{-1}(G)$ (this was done in the case $G = \mathrm{Aut}_{\mathbf{C}}(A)$ in remark 1.3.2(2), the general case is similar). Then, applying lemma 1.4.13, we have that

$$H(A/G) \cong H(A_k/\gamma_\varphi^{-1}(G)) \cong \mathrm{Aut}_{\mathbf{C}}(A_k)/\gamma_\varphi^{-1}(G) \cong \mathrm{Aut}_{\mathbf{C}}(A)/G \, .$$

Lemma 1.4.15. *The functor H defined in 1.4.2 is essentially surjective.*

Proof. Let Z be an object of π-**sets**. We assume first that Z is connected, i.e. that the action of π on Z is transitive. By lemma 1.4.9(3), there exist $k \in J$, $G \leq \mathrm{Aut}_{\mathbf{C}}(A_k)$ such that $Z \cong \mathrm{Aut}_{\mathbf{C}}(A_k)/G$, with the action described as in the lemma. By lemma 1.4.13, we have that $H(A_k/G) \cong \mathrm{Aut}_C(A_k)/G$ (again, the quotient exists by (G2) of the definition of Galois category). Comparing the definitions of the actions that were given in the two lemmas, we see that they agree. Then we have that $Z \cong H(A_k/G)$.
We deal now with the general case. By proposition 1.2.20, we can write $Z = Z_1 \amalg \cdots \amalg Z_n$, with $Z_1, \ldots, Z_n$ connected (this is actually the orbit decomposition, see example 1.2.22). By what we proved above, there exist $X_1, \ldots, X_n$ objects of $\mathbf{C}$ such that $H(X_i) \cong Z_i$ for any $i = 1, \ldots, n$. Then, applying corollary 1.4.12, we get that

$$Z = Z_1 \amalg \cdots \amalg Z_n \cong H(X_1) \amalg \cdots \amalg H(X_n) \cong H\left(X_1 \amalg \cdots \amalg X_n\right) \, .$$

□

It remains to prove that H is full, i.e. that the map

$$\mathrm{Hom}_{\mathbf{C}}(X,Y) \to \mathrm{Hom}_{\pi\textbf{-sets}}(H(X),H(Y)),\ f \mapsto H(f)$$

is surjective for any X, Y objects of $\mathbf{C}$. The following lemmas will allow us to consider only the case when X and Y are both connected.

Lemma 1.4.16. *Let $X_1,\dots,X_n$, Y be objects of $\mathbf{C}$. Let X be the sum of $X_1,\dots,X_n$, together with the morphisms $q_i : X_i \to X$, for $i = 1,\dots,n$. For any $i = 1,\dots,n$, consider the map*

$$\eta_i : \mathrm{Hom}_{\mathbf{C}}(X_i,Y) \to \mathrm{Hom}_{\pi\textbf{-sets}}(H(X_i),H(Y)),\ f \mapsto H(f)\ .$$

The maps $\eta_1,\dots,\eta_n$ induce a map

$$\eta_1 \times \cdots \times \eta_n : \prod_{i=1}^{n} \mathrm{Hom}_{\mathbf{C}}(X_i,Y) \to \prod_{i=1}^{n} \mathrm{Hom}_{\pi\textbf{-sets}}(H(X_i),H(Y)),$$
$$(f_1,\dots,f_n) \mapsto (\eta_1(f_1),\dots,\eta_n(f_n))\ .$$

Moreover, consider the map

$$\eta : \mathrm{Hom}_{\mathbf{C}}(X,Y) \to \mathrm{Hom}_{\pi\textbf{-sets}}(H(X),H(Y)),\ f \mapsto H(f)\ .$$

Then we have a bijection $\varphi : \mathrm{Hom}_{\mathbf{C}}(X,Y) \to \prod_{i=1}^{n} \mathrm{Hom}_{\mathbf{C}}(X_i,Y)$ and a bijection $\psi : \mathrm{Hom}_{\pi\textbf{-sets}}(H(X),H(Y)) \to \prod_{i=1}^{n} \mathrm{Hom}_{\pi\textbf{-sets}}(H(X_i),H(Y))$ such that $\eta = \psi^{-1} \circ (\eta_1 \times \cdots \times \eta_n) \circ \varphi$. In particular, if η_i is surjective for every $i = 1,\dots,n$, then η is also surjective.

Proof. Define

$$\varphi : \mathrm{Hom}_{\mathbf{C}}(X,Y) \to \prod_{i=1}^{n} \mathrm{Hom}_{\mathbf{C}}(X_i,Y),\ f \mapsto (f \circ q_1,\dots,f \circ q_n)\ .$$

We have that φ is bijective by the universal property of the sum. Analogously, define

$$\varphi' : \mathrm{Hom}_{\pi\textbf{-sets}}\left(\coprod_{i=1}^{n} H(X_i),H(Y)\right) \to \prod_{i=1}^{n} \mathrm{Hom}_{\pi\textbf{-sets}}(H(X_i),H(Y)),$$
$$f \mapsto (f \circ q'_1,\dots,f \circ q'_n)\ ,$$

where $q'_j : H(X_j) \to \coprod_{i=1}^{n} H(X_i)$, with $j = 1,\dots,n$, are the canonical inclusions. We have that also φ' is bijective by the universal property of the sum. Since H commutes with finite sums (corollary 1.4.12), we have an isomorphism of π-sets $\vartheta : \coprod_{i=1}^{n} H(X_i) \to H(X)$ such that $\vartheta \circ q'_j = H(q_j)$ for any $j = 1,\dots,n$. We have that ϑ induces the map

$$\vartheta^* : \mathrm{Hom}_{\pi\textbf{-sets}}(H(X),H(Y)) \to \mathrm{Hom}_{\pi\textbf{-sets}}\left(\coprod_{i=1}^{n} H(X_i),H(Y)\right),\ f \mapsto f \circ \vartheta\ ,$$

which is a bijection because ϑ is an isomorphism. Define $\psi = \varphi' \circ \vartheta^*$. Then ψ is a bijection because it is a composition of bijections. Moreover, for any $f \in \mathrm{Hom}_{\mathbf{C}}(X, Y)$ we have

$$(\psi \circ \eta)(f) = \psi(H(f)) = \varphi'(\vartheta^*(H(f))) = \varphi'(H(f) \circ \vartheta) = \\ (H(f) \circ \vartheta \circ q_i')_{i=1,\dots,n} = (H(f) \circ H(q_i))_{i=1,\dots,n} = (H(f \circ q_i))_{i=1,\dots,n} = \\ = (\eta_1 \times \cdots \times \eta_n)\left((f \circ q_i)_{i=1,\dots,n}\right) = ((\eta_1 \times \cdots \times \eta_n) \circ \varphi)(f) .$$

So $\psi \circ \eta = (\eta_1 \times \cdots \times \eta_n) \circ \varphi$, which implies the claim.
Finally, assume that η_i is surjective for any $i = 1, \dots, n$ and let $(g_1, \dots, g_n) \in \prod_{i=1}^n \mathrm{Hom}_{\pi\textbf{-sets}}(H(X_i), H(Y))$. Then for any $i = 1, \dots, n$, since η_i is surjective, there exists $f_i \in \mathrm{Hom}_{\mathbf{C}}(X_i, Y)$ such that $g_i = \eta_i(f_i)$. We have that $(f_1, \dots, f_n) \in \prod_{i=1}^n \mathrm{Hom}_{\mathbf{C}}(X_i, Y)$ and $(g_1, \dots, g_n) = (\eta_1 \times \cdots \times \eta_n)((f_1, \dots, f_n))$. This shows that $\eta_1 \times \cdots \times \eta_n$ is surjective. Hence $\eta = \psi^{-1} \circ (\eta_1 \times \cdots \times \eta_n) \circ \varphi$ is surjective, because it is the composition of surjective maps. □

The following lemma is in a sense the "converse" of lemma 1.4.13: while that lemma told us how to get connected π-sets as images of objects of $\mathbf{C}$, this one shows us what the effect of H on connected objects of $\mathbf{C}$ is. At the same time, it gives a description of connected objects as quotients of Galois objects.

Lemma 1.4.17. *Let B be a connected object of $\mathbf{C}$. Then:*

(1) there exist $k \in J$ and a subgroup $G \leq \mathrm{Aut}_{\mathbf{C}}(A_k)$ (G is finite because A_k is Galois by remark 1.3.12 and so $\mathrm{Aut}_{\mathbf{C}}(A_k)$ is finite by remark 1.3.2(1)) such that $H(B) \cong \mathrm{Aut}_{\mathbf{C}}(A_k)/G$, with the action given by $\sigma(\tau G) = (\sigma_k \tau)G$, for any $\sigma = (\sigma_j)_{j \in J} \in \pi = \varprojlim_{j \in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$, $\tau \in \mathrm{Aut}_{\mathbf{C}}(A_j)/G$ (this is the same as in lemma 1.4.9(3));

(2) $H(B)$ is a connected π-set, i.e. the action of π on the set $H(B) = F(B)$ is transitive (see example 1.2.14(2));

(3) $B \cong A_k/G$, where k and G are as in point (1).

Proof. (1) By lemma 1.3.5, there exists a pair $(A, a) \in \mathcal{I}$ such that A is Galois and $\psi^B_{(A,a)} : \mathrm{Hom}_{\mathbf{C}}(A, B) \to F(B)$ is bijective. Define $k := [(A, a)]_\sim$. Since A is Galois, $k \in J$. Since $[(A, a)]_\sim = k = [(A_k, a_k)]_\sim$, we have $(A, a) \sim (A_k, a_k)$, i.e. there exists an isomorphism $\varphi : A \to A_k$ such that $F(\varphi)(a) = a_j$. For any $f \in \mathrm{Hom}_{\mathbf{C}}(A_k, B)$, we have that

$$\psi^B_{(A_k,a_k)}(f) = F(f)(a_k) = F(f)(F(\varphi)(a)) = \\ = F(f \circ \varphi)(a) = \psi^B_{(A,a)}(f \circ \varphi) = \left(\psi^B_{(A,a)} \circ \varphi^*\right)(f) ,$$

where $\varphi^* : \mathrm{Hom}_{\mathbf{C}}(A_k, B) \to \mathrm{Hom}_{\mathbf{C}}(A, B)$, $g \mapsto g \circ \varphi$ is a bijection because φ is an isomorphism. Then $\psi^B_{(A_k,a_k)} = \psi^B_{(A,a)} \circ \varphi^*$ is a bijection, because it is a composition of bijections. Since B is connected, it is not initial (remark 1.2.13(1)). Then $F(B) \neq \emptyset$ (lemma 1.2.17). Since $F(B) \cong \mathrm{Hom}_{\mathbf{C}}(A_k, B)$

via $\psi^B_{(A_k,a_k)}$, we have that $\mathrm{Hom}_{\mathbf{C}}(A_k, B) \neq \emptyset$. By lemma 1.3.13, $\mathrm{Aut}_{\mathbf{C}}(A_k)$ acts transitively on $\mathrm{Hom}_{\mathbf{C}}(A_k, B)$. Since $\psi^B_{(A_k,a_k)}$ is bijective, this induces a transitive action of $\mathrm{Aut}_{\mathbf{C}}(A_k)$ on $F(B)$:

$$\sigma b = \psi^B_{(A_k,a_k)}\left(\sigma.\left(\psi^B_{(A_k,a_k)}\right)^{-1}(b)\right) ,$$

for any $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_k)$, $b \in F(B)$. We claim that this action is compatible with that of π on $F(B) = H(B)$, in the sense that $\sigma b = \sigma_k b$ for any $\sigma = (\sigma_j)_{j\in J} \in \pi = \varprojlim_{j\in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$, $b \in B$. Remember that the action of π on $F(B) = H(B)$ was induced by that on $\varinjlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, B)$ via the bijection $\psi'_B : \varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, B) \to F(B)$ defined as in the proof of proposition 1.2.35, but considering J as index set instead of I. Then we have $\psi'_B([f]_\sim) = \psi^B_{(A_j,a_j)}(f)$ for any $f \in \mathrm{Hom}_{\mathbf{C}}(A_j, B)$, with $j \in J$. Let $b \in B$. Since $\psi^B_{(A_k,a_k)}$ is bijective, there exists a unique $f \in \mathrm{Hom}_{\mathbf{C}}(A_k, B)$ such that $b = \psi^B_{(A_k,a_k)}(f)$. Then we have

$$\psi'_B([f]_\sim) = \psi^B_{(A_k,a_k)}(f) = b .$$

This means that $[f]_\sim = (\psi'_B)^{-1}(b)$. So, if $\sigma = (\sigma_j)_{j\in J} \in \pi = \varprojlim_{j\in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$, we have

$$\begin{aligned}\sigma b = \psi'_B\left(\sigma\left((\psi'_B)^{-1}(b)\right)\right) = \psi'_B\left(\sigma[f]_\sim\right) = \psi'_B\left([f \circ \sigma_k^{-1}]_\sim\right) = \\ = \psi^B_{(A_k,a_k)}(f \circ \sigma_k^{-1}) = \psi^B_{(A_k,a_k)}\left(\sigma.\left(\psi^B_{(A_k,a_k)}\right)^{-1}(b)\right) = \sigma_k b ,\end{aligned}$$

which is what we wanted. Fix now $b_0 \in F(b)$. Then, since the action of $\mathrm{Aut}_{\mathbf{C}}(A_k)$ on $F(B)$ is transitive, we have that $F(B)$ is isomorphic as an $\mathrm{Aut}_{\mathbf{C}}(A_k)$-set to $\mathrm{Aut}_{\mathbf{C}}(A_k)/G$, where $G = \mathrm{Stab}_{\mathrm{Aut}_{\mathbf{C}}(A_k)}(b_0)$ and the action of $\mathrm{Aut}_{\mathbf{C}}(A_k)$ on $\mathrm{Aut}_{\mathbf{C}}(A_k)/G$ is defined by $\sigma(\tau G) = (\sigma\tau)G$ for any $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_k)$, $\tau \in \mathrm{Aut}_{\mathbf{C}}(A_k)/G$ (this is well known by the theory of group actions, but can also be seen as a consequence of lemma 1.4.9, since $\mathrm{Aut}_{\mathbf{C}}(A_k)$ is the projective limit of itself and is finite). More precisely, the following map is an isomorphism of $\mathrm{Aut}_{\mathbf{C}}(A_k)$-sets:

$$\vartheta : \mathrm{Aut}_{\mathbf{C}}(A_k)/G \to F(B),\ \tau G \mapsto \tau b_0 .$$

But $F(B) = H(B)$ is also a π-set and $\mathrm{Aut}_{\mathbf{C}}(A_k)/G$ can be seen as a π-set as in the statement. We claim that ϑ is an isomorphism of π-sets. Since we already know that it is bijective, we only have to prove that it is a morphism of π-sets. Let $\sigma = (\sigma_j)_{j\in J} \in \pi = \varprojlim_{j\in J} \mathrm{Aut}_{\mathbf{C}}(A_j)$ and $\tau G \in \mathrm{Aut}_{\mathbf{C}}(A_k)/G$. Then

$$\vartheta(\sigma(\tau G)) = \vartheta((\sigma_k\tau)G) = (\sigma_k\tau)b_0 = \sigma_k(\tau b_0) = \sigma(\tau b_0) = \sigma\vartheta(\tau G) .$$

This proves that ϑ is a morphism of π-sets. So $H(B) \cong \mathrm{Aut}_{\mathbf{C}}(A_k)/G$ as π-sets.

(2) Let $b_1, b_2 \in H(B)$. Since the action of $\mathrm{Aut}_{\mathbf{C}}(A_k)$ on $F(B) = H(B)$ is transitive, there exists $\tau \in \mathrm{Aut}_{\mathbf{C}}(A_k)$ such that $b_2 = \tau b_1$. By lemma 1.3.16, the projection $p_k : \pi \to \mathrm{Aut}_{\mathbf{C}}(A_k)$ is surjective. Then there exists $\sigma = (\sigma_j)_{j \in J} \in \pi$ such that $\tau = p_k(\sigma) = \sigma_k$. So, by what we proved above, we have $\sigma b_1 = \sigma_k b_1 = \tau b_1 = b_2$. This shows that the action of π on $H(B)$ is transitive.

(3) First of all, notice that the quotient A_k/G exists by (G2) of the definition of Galois category. Let $f_0 = \psi^{-1}_{(A_k,a_k)}(b) \in \mathrm{Hom}_{\mathbf{C}}(A_k, B)$ and let $\sigma \in G$. Since G is a subgroup of $\mathrm{Aut}_{\mathbf{C}}(A_k)$, we have that also $\sigma^{-1} \in G = \mathrm{Stab}_{\mathrm{Aut}_{\mathbf{C}}(A_k)}(b_0)$. Then

$$\psi^B_{(A_k,a_k)}(f_0) = b_0 = \sigma^{-1} b_0 = \\ = \psi^B_{(A_k,a_k)}\left(\sigma^{-1}.\left(\psi^B_{(A_k,a_k)}\right)^{-1}(b_0)\right) = \psi^B_{(A_k,a_k)}(\sigma^{-1}.f_0)\ .$$

Since $\psi^B_{(A_k,a_k)}$ is injective, this implies that $f_0 = \sigma^{-1}.f_0 = f_0 \circ \sigma$. Since this holds for any σ in G, by the universal property of the quotient (definition 1.1.1(5)) there exists a (unique) morphism $\overline{f_0} : A_k/G \to B$ such that $f_0 = \overline{f_0} \circ p$, where $p : A_k \to A_k/G$ is the morphism that appears in the definition of quotient. We claim that $\overline{f_0}$ is an isomorphism. By (G6) of the definition of Galois category, it is enough to prove that $F\left(\overline{f_0}\right) : F(A_k/G) \to F(B)$ is an isomorphism of sets, i.e. a bijection. Since A_k is Galois, it is not initial. Then, since B is connected, lemma 1.3.9 tells us that $F(f_0)$ is surjective. Since $F(f_0) = F\left(\overline{f_0}\right) \circ F(p)$, it follows that $F\left(\overline{f_0}\right)$ is also surjective. Since $F(A_k/G)$ and $F(B)$ are finite sets, if we prove that they have the same cardinality it will follow that $F\left(\overline{f_0}\right)$ is bijective. By lemma 1.4.13, $H(A_k/G)$ is isomorphic as a π-set to $\mathrm{Aut}_{\mathbf{C}}(A_k)/G$, which in turn is isomorphic to $H(B)$ by point (1). Then $H(A_k/G)$ and $H(B)$ are isomorphic as π-sets. In particular, they are isomorphic as sets, so we must have

$$|F(A_k/G)| = |H(A_k/G)| = |H(B)| = |F(B)|$$

(recall that, as sets, $F(X)$ and $H(X)$ coincide, for any object X of $\mathbf{C}$). This ends the proof.

□

Lemma 1.4.18. *Let X, Y be objects of $\mathbf{C}$ with X connected. If $f : X \to Y$ is an epimorphism, then Y is also connected.*

Proof. Let Z be an object of $\mathbf{C}$ and $g : Z \to Y$ a monomorphism. Assume that Z is not initial. We have to prove that g is an isomorphism (see remark 1.2.13(2)). Consider the fibred product $Z \times_Y X$ (which exists by (G1) of the definition of Galois category), with projections $p_1 : Z \times_Y X \to Z$, $p_2 : Z \times_Y X \to X$. By lemma 1.2.15, p_2 is a monomorphism, because g is a monomorphism. Since X is connected, we have that either $Z \times_Y X$ is initial or p_2 is an isomorphism. By (G4) of the definition of Galois category, we have that $F(Z \times_Y X) \cong F(Z) \times_{F(Y)} F(X)$. Since f is an epimorphism, by (G5) of the definition of Galois category we have that

$F(f) : F(X) \to F(Y)$ is an epimorphism of sets, i.e. a surjective map (see example 1.1.3(6)). Since Z is not initial, $F(Z) \neq \emptyset$ (lemma 1.2.17). So there exists $z \in F(Z)$. Then $F(g)(z) \in F(Y)$. Since $F(f)$ is surjective, there exists $x \in F(X)$ such that $F(f)(x) = F(g)(z)$. Then $(z, x) \in F(Z) \times_{F(Y)} F(X)$ (see example 1.1.3(2)). This means that $F(Z) \times_{F(Y)} F(X) \neq \emptyset$ and so $F(Z \times_Y X) \neq \emptyset$, which implies that $Z \times_Y X$ is not initial, by (G5) of the definition of Galois category. So p_2 is an isomorphism. This implies that $F(p_2)$ is an isomorphism of sets, i.e. a bijection. We prove now that $F(g)$ is surjective. Let $y \in F(Y)$. Since $F(f)$ is surjective, there exists $x \in F(X)$ such that $F(f)(x) = y$. Since $F(p_2)$ is a bijection, also the projection $F(Z) \times_{F(Y)} F(X) \to F(X)$ is a bijection, in particular it is surjective. Then there exists $z \in F(Z)$ such that $(z, x) \in F(Z) \times_{F(Y)} F(X)$. This means that $F(g)(z) = F(f)(x) = y$. So $F(g)$ is surjective. But g is a monomorphism, so $F(g)$ is also injective, by corollary 1.2.10. Then $F(g)$ is a bijection, i.e. an isomorphism of sets. By (G6) of the definition of Galois category, g is an isomorphism, which is what we had to prove. □

Lemma 1.4.19. *Let X, Y be objects of $\mathbf{C}$, with X connected. Let $q_1 : Y_1 \to Y, \dots, q_n : Y_n \to Y$ be the connected components of Y. For any $i = 1, \dots, n$, consider the map*

$$\eta_i : \mathrm{Hom}_{\mathbf{C}}(X, Y_i) \to \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y_i)),\ f \mapsto H(f)\ .$$

The maps $\eta_1, \dots, \eta_n$ induce a map

$$\eta' : \coprod_{i=1}^{n} \mathrm{Hom}_{\mathbf{C}}(X, Y_i) \to \coprod_{i=1}^{n} \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y_i)),$$
$$f \mapsto \eta_j(f) \quad \textit{if } f \in \mathrm{Hom}_{\mathbf{C}}(X, Y_j)\ .$$

Moreover, consider the map

$$\eta : \mathrm{Hom}_{\mathbf{C}}(X, Y) \to \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y)),\ f \mapsto H(f)\ .$$

Then we have a bijection $\varphi : \coprod_{i=1}^{n} \mathrm{Hom}_{\mathbf{C}}(X, Y_i) \to \mathrm{Hom}_{\mathbf{C}}(X, Y)$ and a bijection $\psi : \coprod_{i=1}^{n} \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y_i)) \to \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y))$ such that $\eta = \psi \circ \eta' \circ \varphi^{-1}$. In particular, if η_i is surjective for every $i = 1, \dots, n$, then η is also surjective.

Proof. Since H commutes with finite sums (corollary 1.4.12), we have an isomorphism of π-sets $\vartheta : \coprod_{i=1}^{n} H(Y_i) \to H(Y)$ such that $\vartheta \circ q'_j = H(q_j)$ for any $j = 1, \dots, n$, where $q'_j : H(Y_j) \to \coprod_{i=1}^{n} H(Y_i)$ is the canonical inclusion.
Define

$$\varphi : \coprod_{i=1}^{n} \mathrm{Hom}_{\mathbf{C}}(X, Y_i) \to \mathrm{Hom}_{\mathbf{C}}(X, Y),\ f \mapsto q_j \circ f\ ,$$

where j is the unique element of $\{1, \dots, n\}$ such that $f \in \mathrm{Hom}_{\mathbf{C}}(X, Y_j)$. We prove that φ is bijective.
Let $f_1, f_2 \in \coprod_{i=1}^{n} \mathrm{Hom}_{\mathbf{C}}(X, Y_i)$ such that $\varphi(f_1) = \varphi(f_2)$. Let $j_1, j_2 \in \{1, \dots, n\}$ such that $f_1 \in \mathrm{Hom}_{\mathbf{C}}(X, Y_{j_1})$, $f_2 \in \mathrm{Hom}_{\mathbf{C}}(X, Y_{j_2})$. Then $q_{j_1} \circ f_1 = q_{j_2} \circ f_2$. Applying H, we get $H(q_{j_1}) \circ H(f_1) = H(q_{j_2}) \circ H(f_2)$. Then

$$q'_{j_1} \circ H(f_1) = \vartheta^{-1} \circ H(q_{j_1}) \circ H(f_1) = \vartheta^{-1} \circ H(q_{j_2}) \circ H(f_2) = q'_{j_2} \circ H(f_2)\ .$$

In particular, $\mathrm{Im}(q'_{j_1} \circ H(f_1)) = \mathrm{Im}(q'_{j_2} \circ H(f_2))$ (and this image is non-empty, because X connected implies that X is not initial and then $H(X) \neq \emptyset$). But $\mathrm{Im}(q'_{j_1} \circ H(f_1)) \subseteq \mathrm{Im}(q'_{j_1})$ and $\mathrm{Im}(q'_{j_2} \circ H(f_2)) \subseteq \mathrm{Im}(q'_{j_2})$. So $\mathrm{Im}(q'_{j_1}) \cap \mathrm{Im}(q'_{j_2}) \neq \emptyset$, which implies that $j_1 = j_2$ (recall that the sum $\coprod_{i=1}^n H(Y_i)$ is just the disjoint union of the $H(Y_i)$'s, with a suitable action of π, see the proof of proposition 1.1.15). So $q'_{j_1} \circ f_1 = q'_{j_1} \circ f_2$. But q'_{j_1} is a monomorphism by assumption (because it defines a subobject of Y). Then we must have $f_1 = f_2$. So φ is injective.
Let now $f \in \mathrm{Hom}_{\mathbf{C}}(X, Y)$. By (G3) of the definition of Galois category, we can write $f = u' \circ u''$, where $u'' : X \to Z$ is an epimorphism and $u' : Z \to Y$ is a monomorphism. By lemma 1.4.18, Z is connected, because X is connected. Then, by lemma 1.2.19, there exists a unique $j \in \{1, \ldots, n\}$ such that u' is equivalent to q_j. This means that there exists an isomorphism $\alpha : Z \to Y_j$ such that $u' = q_j \circ \alpha$. We have that $\alpha \circ u'' \in \mathrm{Hom}_{\mathbf{C}}(X, Y_j) \subseteq \coprod_{i=1}^n \mathrm{Hom}_{\mathbf{C}}(X, Y_i)$ and $\varphi(\alpha \circ u'') = q_j \circ \alpha \circ u'' = u' \circ u'' = f$. This proves surjectivity.
Define now

$$\varphi' : \coprod_{i=1}^{n} \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y_i)) \to \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}\left(H(X), \coprod_{i=1}^{n} H(Y_i)\right), \ f \mapsto q'_j \circ f \ ,$$

where $j \in \{1, \ldots, n\}$ is such that $f \in \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y_j))$. Recall that π**-sets** is a Galois category (proposition 1.1.15). By lemma 1.4.17(2), $H(X)$ is connected and also $H(Y_j)$ is connected, for any $j = 1, \ldots, n$. Then $q'_1, \ldots, q'_n$ are the connected components of $\coprod_{i=1}^n H(Y_i)$. This means that the same argument that we used to prove that φ is bijective applies also to φ'. Then φ' is bijective. We have that ϑ induces the map

$$\vartheta_* : \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}\left(H(X), \coprod_{i=1}^{n} H(Y_i)\right) \to \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y)), \ f \mapsto \vartheta \circ f \ ,$$

which is a bijection because ϑ is an isomorphism. Define $\psi = \vartheta_* \circ \varphi'$. Then ψ is a bijection because it is a composition of bijections. Moreover, let $f \in \coprod_{i=1}^n \mathrm{Hom}_{\mathbf{C}}(X, Y_i)$ and let $j \in \{1, \ldots, n\}$ be such that $f \in \mathrm{Hom}_{\mathbf{C}}(X, Y_j)$. Then we have

$$\begin{aligned}(\eta \circ \varphi)(f) &= \eta(q_j \circ f) = H(q_j \circ f) = H(q_j) \circ H(f) = \vartheta \circ q'_j \circ H(f) = \\ &= \vartheta \circ \varphi'(H(f)) = \vartheta_*(\varphi'(H(f))) = (\vartheta_* \circ \varphi')(\eta'(f)) = (\psi \circ \eta')(f) \ .\end{aligned}$$

So $\eta \circ \varphi = \psi \circ \eta'$, which implies the claim.
Finally, if η_i is surjective for any $i = 1, \ldots, n$ and $g \in \coprod_{i=1}^n \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y_i))$, there exists a unique $j \in \{1, \ldots, n\}$ such that $g \in \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y_j))$. Then, since η_j is surjective, there exists $f \in \mathrm{Hom}_{\mathbf{C}}(H, Y_j) \subseteq \coprod_{i=1}^n \mathrm{Hom}_{\mathbf{C}}(X, Y_i)$ such that $g = \eta_j(f) = \eta'(f)$. This shows that η' is surjective. Hence $\eta = \psi \circ \eta' \circ \varphi^{-1}$ is surjective, because it is the composition of surjective maps. □

Lemma 1.4.20. *The functor H defined in 1.4.2 is full.*

Proof. Let X, Y be objects of $\mathbf{C}$. We have to prove that the map

$$\mathrm{Hom}_{\mathbf{C}}(X, Y) \to \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y)), \ f \mapsto H(f)$$

is surjective. By proposition 1.2.20, we can write $X = \coprod_{i=1}^{n} X_i$, where $X_i \to X$ with $i = 1, \dots, n$ are the connected components of X. Then by lemma 1.4.16 it is enough to prove that the map $\mathrm{Hom}_{\mathbf{C}}(X_i, Y) \to \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X_i), H(Y)),\ f \mapsto H(f)$ is surjective for any $i = 1, \dots, n$. So we can assume without loss of generality that X is connected.
Again by proposition 1.2.20, we can write $Y = \coprod_{j=1}^{m} Y_i$, where $Y_j \to Y$ with $j = 1, \dots, m$ are the connected components of Y. Then by lemma 1.4.19 it is enough to prove that the map $\mathrm{Hom}_{\mathbf{C}}(X, Y_j) \to \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y_j)),\ f \mapsto H(f)$ is surjective for any $j = 1, \dots, m$. So we can assume without loss of generality that also Y is connected.
Notice that $\mathrm{Hom}_{\mathbf{C}}(X, Y)$ is finite. Indeed, since X is connected we have that $\psi^{Y}_{(X,x)} : \mathrm{Hom}_{\mathbf{C}}(X, Y) \to F(Y)$ is injective, where x is any element of $F(X)$ (which is non-empty because X connected implies that X is not initial, see remark 1.2.13(1) and lemma 1.2.17). Then $|\mathrm{Hom}_{\mathbf{C}}(X, Y)| \leq |F(Y)| < +\infty$. By corollary 1.4.8, we know that the map $\mathrm{Hom}_{\mathbf{C}}(X, Y) \to \mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y))$ is injective. Then, in order to show that it is surjective, it is enough to show that $|\mathrm{Hom}_{\mathbf{C}}(X, Y)| = |\mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y))|$.
By lemma 1.4.17, there exist $k_1, k_2 \in J$, $G_1 \leq \mathrm{Aut}_{\mathbf{C}}(A_{k_1})$, $G_2 \leq \mathrm{Aut}_{\mathbf{C}}(A_{k_2})$ such that $X \cong A_{k_1}/G_1$ and $Y \cong A_{k_2}/G_2$. Since J is directed (lemma 1.3.10), there exists $k \in J$ such that $k \geq k_1$ and $k \geq j_2$. Define $L_1 := \rho^{-1}_{kk_1}(G_1) \leq \mathrm{Aut}_{\mathbf{C}}(A_k)$ and $L_2 := \rho^{-1}_{kk_2}(G_2) \leq \mathrm{Aut}_{\mathbf{C}}(A_k)$. By (G2) of the definition of Galois category, the quotients A_k/L_1 and A_k/L_2 exist in $\mathbf{C}$. Denote by $p_1 : A_{k_1} \to A_{k_1}/G_1$, $p_2 : A_{k_2} \to A_{k_2}/G_2$, $q_1 : A_k \to A_k/L_1$, $q_2 : A_k \to A_k/L_2$ the morphisms that appear in the definition of the quotients. Consider the morphism $p_1 \circ f_{kk_1} : A_k \to A_{k_1}/G_1$. Let $\sigma \in L_1 = \rho^{-1}_{kk_1}(G_1)$. Then $\rho_{kk_1}(\sigma) \in G_1$ and this implies that $p_1 \circ \rho_{kk_1}(\sigma) = p_1$ (definition of quotient). By definition of ρ_{kk_1} (proposition 1.3.14), we have that

$$p_1 \circ f_{kk_1} \circ \sigma = p_1 \circ \rho_{kk_1}(\sigma) \circ f_{kk_1} = p_1 \circ f_{kk_1} .$$

Since this holds for any $\sigma \in L_1$, by the universal property of the quotient there exists a morphism $\varphi : A_k/L_1 \to A_{k_1}/G_1$ such that $p_1 \circ f_{kk_1} = \varphi \circ q_1$. We claim that φ is an isomorphism. By (G6) of the definition of Galois category, it is enough to prove that $F(\varphi) : F(A_k/L_1) \to F(A_{k_1}/G_1)$ is an isomorphism of sets, i.e. a bijection. We have that $A_{k_1}/G_1 \cong X$ is connected. Then, by lemma 1.3.9, $F(\varphi)$ is surjective. Since the sets are finite, in order to prove that $F(\varphi)$ is bijective it is enough to show that they have the same cardinality. As sets, we have that $F(A_k/L_1) = H(A_k/L_1) \cong \mathrm{Aut}_{\mathbf{C}}(A_k)/L_1$ and $F(A_{k_1}/G_1) = H(A_{k_1}/G_1) \cong \mathrm{Aut}_{\mathbf{C}}(A_{k_1})/G_1$ (see lemma 1.4.13). Using the fact that ρ_{kk_1} is surjective, it is immediate to prove that the following map is well-defined and bijective:

$$\mathrm{Aut}_{\mathbf{C}}(A_k)/L_1 \to \mathrm{Aut}_{\mathbf{C}}(A_{k_1})/G_1,\ \sigma L_1 \mapsto \rho_{kk_1}(\sigma) G_1 .$$

Then $|\mathrm{Aut}_{\mathbf{C}}(A_k)/L_1| = |\mathrm{Aut}_{\mathbf{C}}(A_{k_1})/G_1|$. So $X \cong A_{k_1}/G_1 \cong A_k/L_1$. In the same way, one can show that $Y \cong A_{k_2}/G_2 \cong A_k/L_2$. These isomorphisms induce a bijection between $\mathrm{Hom}_{\mathbf{C}}(X, Y)$ and $\mathrm{Hom}_{\mathbf{C}}(A_k/L_1, A_k/L_2)$. In particular, we have that $|\mathrm{Hom}_{\mathbf{C}}(X, Y)| = |\mathrm{Hom}_{\mathbf{C}}(A_k/L_1, A_k/L_2)|$. Applying lemma 1.4.13, we have that $H(X) \cong H(A_k/L_1) \cong \mathrm{Aut}_{\mathbf{C}}(A_k)/L_1$ and $H(Y) \cong H(A_k/L_2) \cong$

$\mathrm{Aut}_{\mathbf{C}}(A_k)/L_2$. Then we have a bijection between $\mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y))$ and $\mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(\mathrm{Aut}_{\mathbf{C}}(A_k)/L_1, \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2)$. So

$$|\mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(H(X), H(Y))| = |\mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(\mathrm{Aut}_{\mathbf{C}}(A_k)/L_1, \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2)| \ .$$

Then what we have to prove is that

$$|\mathrm{Hom}_{\mathbf{C}}(A_k/L_1, A_k/L_2)| = |\mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(\mathrm{Aut}_{\mathbf{C}}(A_k)/L_1, \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2)| \ .$$

Let us count how many morphisms of π-sets we have between $\mathrm{Aut}_{\mathbf{C}}(A_k)/L_1$ and $\mathrm{Aut}_{\mathbf{C}}(A_k)/L_2$. Notice that, by definition of the action of π and using the fact that $p_k : \pi \to \mathrm{Aut}_{\mathbf{C}}(A_k)$ is surjective (lemma 1.3.16), a map $f : \mathrm{Aut}_{\mathbf{C}}(A_k)/L_1 \to \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2$ is a morphism of π-sets if and only if it is a morphism of $\mathrm{Aut}_{\mathbf{C}}(A_k)$-sets. Let $f : \mathrm{Aut}_{\mathbf{C}}(A_k)/L_1 \to \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2$ be a morphism of $\mathrm{Aut}_{\mathbf{C}}(A_k)$-sets and consider $\sigma L_1 \in \mathrm{Aut}_{\mathbf{C}}(A_k)/L_1$. Then $f(\sigma L_1) = f(\sigma(L_1)) = \sigma f(L_1)$, since f is a morphism of $\mathrm{Aut}_{\mathbf{C}}(A_k)$-sets. This shows that f is uniquely determined by $f(L_1)$. Since $f(L_1) \in \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2$, there exists $\tau \in \mathrm{Aut}_{\mathbf{C}}(A_k)$ such that $f(L_1) = \tau L_2$. For any $\sigma \in L_1$, we have $\sigma L_1 = L_1$ and so

$$\tau L_2 = f(L_1) = f(\sigma L_1) = \sigma f(L_1) = \sigma(\tau L_2) = (\sigma\tau)L_2 \ .$$

This means that $\tau^{-1}\sigma\tau \in L_2$.
On the other hand, let $\tau L_2 \in \mathrm{Aut}_{\mathbf{C}}(A_k)$ be such that $\tau^{-1}\sigma\tau \in L_2$ for any $\sigma \in L_1$. Notice that this condition does not depend on the representative we choose. Indeed, if $\tau' \in \mathrm{Aut}_{\mathbf{C}}(A_k)$ is such that $\tau L_2 = \tau' L_2$, then there exists $\tau_0 \in L_2$ such that $\tau' = \tau\tau_0$ and so $(\tau')^{-1}\sigma\tau' = \tau_0^{-1}(\tau^{-1}\sigma\tau)\tau_0 \in L_2$, because L_2 is a subgroup of $\mathrm{Aut}_{\mathbf{C}}(A_k)$. Define

$$f_{\tau L_2} : \mathrm{Aut}_{\mathbf{C}}(A_k)/L_1 \to \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2,\ \sigma L_1 \mapsto (\sigma\tau)L_2 \ .$$

We have that $f_{\tau L_2}$ is well defined. Indeed, if $\sigma_1 L_1 = \sigma_2 L_2$, with $\sigma_1, \sigma_2 \in \mathrm{Aut}_{\mathbf{C}}(A_k)$, then $\sigma_2^{-1}\sigma_1 \in L_1$ and so $(\sigma_2\tau)^{-1}(\sigma_1\tau) = \tau^{-1}\sigma_2^{-1}\sigma_1\tau \in L_2$ by the assumption on τL_2. This means that $(\sigma_1\tau)L_2 = (\sigma_2\tau)L_2$. Clearly, $f_{\tau L_2}(L_1) = \tau L_2$. Moreover, $f_{\tau L_2}$ is a morphism of $\mathrm{Aut}_{\mathbf{C}}(A_k)$-sets. Indeed, if $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_k)$ and $\sigma' L_1 \in \mathrm{Aut}_{\mathbf{C}}(A_k)/L_1$, we have that

$$\begin{aligned} f_{\tau L_2}(\sigma(\sigma' L_1)) = f_{\tau L_2}((\sigma\sigma')L_1) = ((\sigma\sigma')\tau)L_2 = \\ = (\sigma(\sigma'\tau))L_2 = \sigma((\sigma'\tau)L_2) = \sigma f_{\tau L_2}(\sigma' L_1) \ . \end{aligned}$$

So, if $\tau L_2 \in \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2$ satisfies $\tau^{-1}\sigma\tau \in L_2$ for any $\sigma \in L_1$, we have a morphism of $\mathrm{Aut}_{\mathbf{C}}(A_k)$-sets sending L_1 into τL_2.This shows that

$$\begin{aligned} &|\mathrm{Hom}_{\pi\text{-}\mathbf{sets}}(\mathrm{Aut}_{\mathbf{C}}(A_k)/L_1, \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2)| = \\ &= |\mathrm{Hom}_{\mathrm{Aut}_{\mathbf{C}}(A_k)}(\mathrm{Aut}_{\mathbf{C}}(A_k)/L_1, \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2)| = \\ &= |\{\tau L_2 \in \mathrm{Aut}_{\mathbf{C}}(A_k)/L_2 : \forall\sigma \in L_1 \quad \tau^{-1}\sigma\tau \in L_2\}| \ . \end{aligned}$$

We count now the number of morphisms between A_k/L_1 and A_k/L_2. Let $f : A_k/L_1 \to A_k \to L_2$ be a morphism in $\mathbf{C}$. Consider the following diagram.

$$\begin{array}{ccc} A_k & \xrightarrow{q_1} & A_k/L_1 \\ \Big\downarrow{?} & & \Big\downarrow{f} \\ A_k & \xrightarrow{q_2} & A_k/L_2 \end{array}$$

By uniqueness in the universal property of the quotient, f is uniquely determined by the composition $f \circ q_1$. We have that $A_k/L_2 \cong Y$ is connected, so $F(q_2) : F(A_k) \to F(A_k/L_2)$ is surjective by lemma 1.3.9. Then there exists $a' \in F(A_k)$ such that $F(q_2)(a') = F(f \circ q_1)(a_k)$. Since A_k is Galois, the action of $\mathrm{Aut}_{\mathbf{C}}(A_k)$ on $F(A_k)$ is transitive (lemma 1.3.4). Then there exists $\tau \in \mathrm{Aut}_{\mathbf{C}}(A_k)$ such that $a' = \tau a_k = F(\tau)(a_k)$. So we have

$$\psi^{A_k/L_2}_{(A_k,a_k)}(f \circ q_1) = F(f \circ q_1)(a_k) = F(q_2)(a') = \\ = F(q_2)(F(\tau)(a_k)) = F(q_2 \circ \tau)(a_k) = \psi^{A_k/L_2}_{(A_k,a_k)}(q_2 \circ \tau) \ .$$

Since $\psi^{A_k/L_2}_{(A_k,a_k)}$ is injective (lemma 1.2.30), this implies that $f \circ q_1 = q_2 \circ \tau$. Let $\tau' \in \mathrm{Aut}_{\mathbf{C}}(A_k)$. We have that $q_2 \circ \tau' = f \circ q_1 = q_2 \circ \tau$ if and only if

$$F(q_2 \circ \tau')(a_k) = \psi^{A_k/L_2}_{(A_k,a_k)}(q_2 \circ \tau') = \psi^{A_k/L_2}_{(A_k,a_k)}(q_2 \circ \tau) = F(q_2 \circ \tau)(a_k)$$

(the "only if" follows from the injectivity of $\psi^{A_k/L_2}_{(A_k,a_k)}$). By (G5) of the definition of Galois category, there exists a bijection

$$\vartheta : F(A_k/L_2) \to F(A_k)/F(L_2)$$

such that $\vartheta \circ F(q_2) = q$, where $q : F(A_k) \to F(A_k)/F(L_2)$, $x \mapsto F(L_2)x$ is the projection on the set of orbits. Then we have that $F(q_2 \circ \tau')(a_k) = F(q_2 \circ \tau)(a_k)$ if and only if $\vartheta(F(q_2 \circ \tau')(a_k)) = \vartheta(F(q_2 \circ \tau)(a_k))$, i.e. if and only if

$$F(L_2)F(\tau')(a_k) = q(F(\tau')(a_k)) = q(F(\tau)(a_k)) = F(L_2)F(\tau)(a_k) \ .$$

This happens if and only if there exists $\sigma \in L_2$ such that

$$F(\tau')(a_k) = F(\sigma)(F(\tau)(a_k)) = F(\sigma\tau)(a_k) \ .$$

But this means that $\psi^{A_k}_{(A_k,a_k)}(\tau') = \psi^{A_k}_{(A_k,a_k)}(\sigma\tau)$ and this is true if and only if $\tau' = \sigma\tau$, by injectivity of $\psi^{A_k}_{(A_k,a_k)}$. Hence we proved that $q_2 \circ \tau' = f \circ q_1$ if and only if $\tau' \in L_2\tau$. So f is uniquely determined by the right coset $L_2\tau$ and different cosets give rise to different morphisms. In the rest of the proof, we will denote by $L_2\backslash \mathrm{Aut}_{\mathbf{C}}(A_k)$ the set of right cosets.

Let $\sigma \in L_1$. By definition of quotient, we have that $q_1 \circ \sigma = q_1$. Then $q_2 \circ \tau \circ \sigma = f \circ q_1 \circ \sigma = f \circ q_1$, which implies that $L_2(\tau\sigma) = L_2\tau$, by what we proved above. This means that $\tau\sigma\tau^{-1} \in L_2$.

On the other hand, let $L_2\tau \in L_2\backslash \mathrm{Aut}_{\mathbf{C}}(A_k)$ be such that $\tau\sigma\tau^{-1} \in L_2$ for any $\sigma \in L_1$ (the fact that this does not depend on the representative can be proved as above). Let $\sigma \in L_1$. Then, since $\tau\sigma\tau^{-1} \in L_2$, we have that $q_2 \circ (\tau\sigma\tau^{-1}) = q_2$, by definition of the quotient. This means that $(q_2 \circ \tau) \circ \sigma = q_2 \circ \tau$. Since this holds for any $\sigma \in L_1$, there exists a unique $f : A_k/L_1 \to A_k/L_2$ such that $q_2 \circ \tau = f \circ q_1$. This shows that

$$|\operatorname{Hom}_{\mathbf{C}}(A_k/L_1, A_k/L_2)| = |\{L_2\tau \in L_2\backslash \operatorname{Aut}_{\mathbf{C}}(A_k) : \forall \sigma \in L_1 \quad \tau\sigma\tau^{-1} \in L_2\}| \,.$$

To finish the proof, define $U := \{\tau L_2 \in \operatorname{Aut}_{\mathbf{C}}(A_k)/L_2 : \forall \sigma \in L_1 \quad \tau^{-1}\sigma\tau \in L_2\}$ and $V := \{L_2\tau \in L_2\backslash \operatorname{Aut}_{\mathbf{C}}(A_k) : \forall \sigma \in L_1 \quad \tau\sigma\tau^{-1} \in L_2\}$ and consider the map

$$\alpha : U \to V,\ \tau L_2 \mapsto L_2\tau^{-1} \,.$$

Let us check that this is well defined. First of all, if $\tau_1 L_2 = \tau_2 L_2$, with $\tau_1, \tau_2 \in \operatorname{Aut}_{\mathbf{C}}(A_k)$, then we have $(\tau_2^{-1})(\tau_1^{-1})^{-1} = \tau_2^{-1}\tau_1 \in L_2$ and so $L_2\tau_1^{-1} = L_2\tau_2^{-1}$. Moreover, if $\tau L_2 \in U$, then for any $\sigma \in L_1$ we have $(\tau^{-1})\sigma(\tau^{-1})^{-1} = \tau^{-1}\sigma\tau \in L_2$. This shows that $L_2\tau^{-1} \in V$. So α is well defined. In the same way, one shows that the map

$$\beta : V \to U,\ L_2\tau \mapsto \tau^{-1}L_2$$

is well defined. It is clear that α and β are inverse to each other. Hence $|U| = |V|$, which is what we needed. □

Proposition 1.4.21. *The functor H defined in 1.4.2 is an equivalence of categories.*

Proof. It follows immediately from 1.4.5, 1.4.8, 1.4.15 and 1.4.20. □

Now we know that any essentially small category is equivalent to the category of finite sets with an action of a certain profinite group. One thing is still missing: uniqueness of this profinite group up to isomorphism. In order to prove this uniqueness, we will consider another profinite group which acts in a natural way on $F(X)$ for any object X. Recall the definition of the automorphism group of a functor.

Definition 1.4.22. Let $\mathbf{C}_1$, $\mathbf{C}_2$ be categories and let $G : \mathbf{C}_1 \to C_2$ be a functor. An *automorphism* of G is an isomorphism of functors $G \to G$, i.e. a collection of isomorphisms $\sigma_X : G(X) \to G(X)$, for each object X of $\mathbf{C}_1$, such that for any morphism $f : X_1 \to X_2$ in $\mathbf{C}_1$ the following diagram is commutative.

$$\begin{array}{ccc} G(X_1) & \xrightarrow{\sigma_{X_1}} & G(X_1) \\ {\scriptstyle G(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ G(X_2) & \xrightarrow{\sigma_{X_2}} & G(X_2) \end{array}$$

Remark 1.4.23. Let $\mathbf{C}_1$, $\mathbf{C}_2$ be categories and let $G : \mathbf{C}_1 \to C_2$ be a functor.

(1) Automorphisms of G can be composed in an obvious way: if $\sigma = (\sigma_X)_{X \in \mathrm{Ob}(\mathbf{C}_1)}$ and $\tau = (\tau_X)_{X \in \mathrm{Ob}(\mathbf{C}_1)}$ are automorphisms of G, then we define $\sigma\tau = (\sigma_X \circ \tau_X)_{X \in \mathrm{Ob}(\mathbf{C}_1)}$ and it is immediate to check that $\sigma\tau$ is indeed an automorphism of G. It is clear that this composition is associative. Moreover, we define $\mathrm{id}_G = (\mathrm{id}_X)_{X \in \mathrm{Ob}(\mathbf{C}_1)}$, which is obviously an automorphism of G and satisfies $\sigma\,\mathrm{id}_G = \sigma = \mathrm{id}_G\,\sigma$ for any automorphism σ of G. Finally, for any automorphism σ of G we can define $\sigma^{-1} = \big((\sigma_X)^{-1}\big)_{X \in \mathrm{Ob}(\mathbf{C}_1)}$, which is easily checked to be an automorphism of G and to satisfy $\sigma\sigma^{-1} = \mathrm{id}_X = \sigma^{-1}\sigma$.

(2) If $\mathbf{C}_1$ is not essentially small, an automorphism of G contains too much data to be a set: it is a proper class. So we cannot consider the class of all automorphisms of G, much less the set of all automorphisms of G. Then, in spite of the properties verified in point (1), we cannot talk of the automorphism group of G. If instead $\mathbf{C}_1$ is essentially small, then the automorphisms of G form a set. Indeed, if we denote by I the set of isomorphism classes of objects of $\mathbf{C}_1$ and we fix a representative X_i for each $i \in I$, an automorphism $\sigma = (\sigma_X)_{X \in \mathrm{Ob}(\mathbf{C}_1)}$ of G is uniquely determined by $(\sigma_{X_i})_{i \in I}$, which can be seen as an element of the product $\prod_{i \in I} \mathrm{Aut}_{\mathbf{C}_2}(G(X_i))$, which is a set. In this case, we denote by $\mathrm{Aut}(G)$ the set of all automorphisms of G, which is a group by point (1).

(3) If $\mathbf{C}_1$ is essentially small, we consider on $\mathrm{Aut}(G)$ the topology which has as a subbase
$$\left\{ f_Y^{-1}(\{\sigma\}) \mid Y \in \mathrm{Ob}(\mathbf{C}_1),\ \sigma \in \mathrm{Aut}_{\mathbf{C}_2}(G(Y)) \right\} ,$$
where we defined $f_Y : \mathrm{Aut}(G) \to \mathrm{Aut}_{\mathbf{C}_2}(G(Y))$, $(\sigma_X)_{X \in \mathrm{Ob}(\mathbf{C}_1)} \mapsto \sigma_Y$ for any object Y of $\mathbf{C}_1$. This is the coarsest topology such that f_Y is continuous for any Y, if we consider the discrete topology on $\mathrm{Aut}_{\mathbf{C}_2}(G(Y))$. Moreover, it can be easily proved that $\mathrm{Aut}(G)$ with this topology is a topological group (i.e. the group's multiplication and inverse are continuous functions).

Lemma 1.4.24. *Let $\mathbf{C}_1$, $\mathbf{C}_2$,$\mathbf{C}_3$ be categories and $G_1 : \mathbf{C}_1 \to \mathbf{C}_2$, $G_2 : \mathbf{C}_2 \to \mathbf{C}_3$ functors. If G_1 is an equivalence of categories, then there is an isomorphism of topological groups between* $\mathrm{Aut}(G_2)$ *and* $\mathrm{Aut}(G_2 \circ G_1)$*.*

Proof. Define
$$\varphi : \mathrm{Aut}(G_2) \to \mathrm{Aut}(G_2 \circ G_1),\ \sigma = (\sigma_Y)_{Y \in \mathrm{Ob}(\mathbf{C}_2)} \mapsto (\sigma_{G_1(X)})_{X \in \mathrm{Ob}(\mathbf{C}_1)} .$$
First of all, we have to check that φ is well defined, i.e. that if $\sigma = (\sigma_Y)_{Y \in \mathrm{Ob}(\mathbf{C}_2)}$ is an automorphism of G_2 then $\varphi(\sigma) = (\sigma_{G_1(X)})_{X \in \mathrm{Ob}(\mathbf{C}_1)}$ is an automorphism of $G_2 \circ G_1$. Let $\sigma = (\sigma_Y)_{Y \in \mathrm{Ob}(\mathbf{C}_2)} \in \mathrm{Aut}(G_2)$. For any object X of $\mathbf{C}_1$, we have that $G_1(X)$ is an object of $\mathbf{C}_2$ and so $\sigma_{G_1(X)} : G_2(G_1(X)) = (G_2 \circ G_1)(X) \to G_2(G_1(X)) = (G_2 \circ G_1)(X)$ is an isomorphism. We have to check that the compatibility condition is satisfied. Let $f : X_1 \to X_2$ be a morphism in $\mathbf{C}_1$. Then $G_1(f) : G_1(X_1) \to G_1(X_2)$ is a morphism in $\mathbf{C}_2$. Since σ is an automorphism of G_2, we have that $G_2(G_1(f)) \circ \sigma_{G_1(X_1)} = \sigma_{G_1(X_2)} \circ G_2(G_1(f))$. Since $G_2(G_1(f)) = (G_2 \circ G_1)(f)$, this shows that $\varphi(\sigma)$ is an automorphism of $G_2 \circ G_1$.
We prove now that φ is a group homomorphism. Let $\sigma = (\sigma_Y)_{Y \in \mathrm{Ob}(\mathbf{C}_2)}, \tau = (\tau_Y)_{Y \in \mathrm{Ob}(\mathbf{C}_2)} \in \mathrm{Aut}(G_2)$. Then
$$\begin{aligned}\varphi(\sigma\tau) = \varphi\left((\sigma_Y \circ \tau_Y)_{Y \in \mathrm{Ob}(\mathbf{C}_2)}\right) = (\sigma_{G_1(X)} \circ \tau_{G_1(X)})_{X \in \mathrm{Ob}(\mathbf{C}_1)} = \\ = (\sigma_{G_1(X)})_{X \in \mathrm{Ob}(\mathbf{C}_1)} (\tau_{G_1(X)})_{X \in \mathrm{Ob}(\mathbf{C}_1)} = \varphi(\sigma)\varphi(\tau) .\end{aligned}$$
So φ is a group homomorphism. We check now that φ is continuous. For any object X_0 of $\mathbf{C}_1$, define
$$f_{X_0} : \mathrm{Aut}(G_2 \circ G_1) \to \mathrm{Aut}_{\mathbf{C}_3}((G_2 \circ G_1)(X_0)),\ (\sigma_X)_{X \in \mathrm{Ob}(\mathbf{C}_1)} \mapsto \sigma_{X_0} .$$

Analogously, for any object Y_0 of $\mathbf{C}_2$, define

$$g_{Y_0} : \mathrm{Aut}(G_2) \to \mathrm{Aut}_{\mathbf{C}_3}(G_2(Y_0)),\ (\sigma_Y)_{Y\in\mathrm{Ob}(\mathbf{C}_2)} \mapsto \sigma_{Y_0} .$$

If X_0 is an object of $\mathbf{C}_1$, by definition of φ we have that $f_{X_0}\circ\varphi = g_{G(X_0)}$. For any object X_0 of $\mathbf{C}_1$ and for any $\sigma \in \mathrm{Aut}_{\mathbf{C}_3}((G_2\circ G_1)(X_0))$, we have that $\varphi^{-1}(f_{X_0}^{-1}(\{\sigma\})) = (f_{X_0}\circ\varphi)^{-1}(\{\sigma\}) = g_{G(X_0)}^{-1}(\{\sigma\})$, which is open by the definition of the topology on $\mathrm{Aut}(G_2)$ (see remark 1.4.23(3)). So φ is continuous.
Let us prove now that φ is bijective. Let $\sigma = (\sigma_Y)_{Y\in\mathrm{Ob}(\mathbf{C}_2)} \in \mathrm{Ker}(\varphi)$. Then

$$(\mathrm{id}_{(G_2\circ G_1)(X)})_{X\in\mathrm{Ob}_{\mathbf{C}_1}} = 1_{\mathrm{Aut}(G_2\circ G_1)} = \varphi(\sigma) = (\sigma_{G_1(X)})_{X\in\mathrm{Ob}(\mathbf{C}_1)} .$$

This means that $\mathrm{id}_{(G_2\circ G_1)(X)} = \sigma_{G_1(X)}$ for any object X of $\mathbf{C}_1$. Let Y be an object of $\mathbf{C}_2$. By lemma 1.4.5, G_1 is essentially surjective. Then there exists an object X of $\mathbf{C}_1$ such that $Y \cong G_1(X)$. Let $\alpha : G_1(X) \to Y$ be an isomorphism. Then $G_2(\alpha)$ is also an isomorphism. Since σ is an automorphism of G_2, we have that

$$\sigma_Y \circ G_2(\alpha) = G_2(\alpha)\circ\sigma_{G_1(X)} = G_2(\alpha)\circ\mathrm{id}_{(G_2\circ G_1)(X)} = G_2(\alpha) .$$

Then $\sigma_Y = G_2(\alpha)\circ G_2(\alpha)^{-1} = \mathrm{id}_Y$. So $\sigma = (\mathrm{id}_Y)_{Y\in\mathrm{Ob}(\mathbf{C}_2)} = 1_{\mathrm{Aut}(G_2)}$. This proves that φ is injective.
Let $\tau = (\tau_X)_{X\in\mathrm{Ob}(\mathbf{C}_1)} \in \mathrm{Aut}(G_2\circ G_1)$. Let $Y \in \mathrm{Ob}(\mathbf{C}_2)$. Since G_1 is essentially surjective, there exists an object X_Y of $\mathbf{C}_1$ such that $Y \cong G_1(X_Y)$. Let $\alpha_Y : G_1(X_Y) \to Y$ be an isomorphism. Then $G_2(\alpha_Y) : (G_2\circ G_1)(X_Y) \to G_2(Y)$ is also an isomorphism. Moreover, $\tau_{X_Y} : (G_2\circ G_1)(X_Y) \to (G_2\circ G_1)(X_Y)$ is an isomorphism, because τ is an automorphism of $G_2\circ G_1$. Define

$$\sigma_Y := G_2(\alpha_Y)\circ\tau_{X_Y}\circ G_2(\alpha_Y)^{-1} : G_2(Y) \to G_2(Y) .$$

Then σ_Y is an isomorphism, because it is a composition of isomorphisms. Let us show that σ_Y does not depend on the choice of X_Y. Let X'_Y be an object of $\mathbf{C}_1$ such that $Y \cong G_1(X'_Y)$, with isomorphism $\alpha'_Y : G_1(X'_Y) \to Y$. Then $\alpha_Y^{-1}\circ\alpha'_Y : G_1(X'_Y) \to G_1(X_Y)$ is an isomorphism in $\mathbf{C}_2$. Since G_1 is an equivalence of categories, it is fully faithful, by lemma 1.4.5. Then there exists a (unique) morphism $f : X'_Y \to X_Y$ such that $G_1(f) = \alpha_Y^{-1}\circ\alpha'_Y$. Since τ is an isomorphism of $G_2\circ G_1$, we have that

$$\begin{aligned}\tau_{X_Y}\circ G_2(\alpha_Y)^{-1}\circ G_2(\alpha'_Y) &= \tau_{X_Y}\circ G_2(\alpha_Y^{-1}\circ\alpha'_Y) = \tau_{X_Y}\circ(G_2\circ G_1)(f) = \\ &= (G_2\circ G_1)(f)\circ\tau_{X'_Y} = G_2(\alpha_Y^{-1}\circ\alpha'_Y)\circ\tau_{X'_Y} = G_2(\alpha_Y)^{-1}\circ G_2(\alpha'_Y)\circ\tau_{X'_Y} .\end{aligned}$$

This implies that $G_2(\alpha_Y)\circ\tau_{X_Y}\circ G_2(\alpha_Y)^{-1} = G_2(\alpha'_Y)\circ\tau_{X'_Y}\circ G_2(\alpha'_Y)^{-1}$. So σ_Y is well defined, because it does not depend on the choice of X_Y. Let now $g : Y_1 \to Y_2$ be a morphism in $\mathbf{C}_2$. As above, we have two objects X_{Y_1}, X_{Y_2} of $\mathbf{C}_1$ with isomorphisms $\alpha_{Y_1} : G_1(X_{Y_1}) \to Y_1$ and $\alpha_{Y_2} : G_1(X_{Y_2}) \to Y_2$. Consider the morphism $\alpha_{Y_2}^{-1}\circ g\circ\alpha_{Y_1} : G_1(X_{Y_1}) \to G_1(X_{Y_2})$. Since G_1 is fully faithful, there exists a unique $f : X_{Y_1} \to X_{Y_2}$ such that $G_1(f) = \alpha_{Y_2}^{-1}\circ g\circ\alpha_{Y_1}$. Since τ is an automorphism of $G_2\circ G_1$, we have that

$$\begin{aligned}\tau_{X_{Y_2}}\circ G_2(\alpha_{Y_2})^{-1}\circ G_2(g)\circ G_2(\alpha_{Y_1}) &= \tau_{X_{Y_2}}\circ G_2(\alpha_{Y_2}^{-1}\circ g\circ\alpha_{Y_1}) = \tau_{X_{Y_2}}\circ(G_2\circ G_1)(f) = \\ = (G_2\circ G_1)(f)\circ\tau_{X_{Y_1}} &= G_2(\alpha_{Y_2}^{-1}\circ g\circ\alpha_{Y_1})\circ\tau_{X_1} = G_2(\alpha_{Y_2})^{-1}\circ G_2(g)\circ G_2(\alpha_{Y_1})\circ\tau_{X_1} .\end{aligned}$$

This implies that

$$\begin{aligned}\sigma_{Y_2} \circ G_2(g) = G_2(\alpha_{Y_2}) \circ \tau_{X_{Y_2}} \circ G_2(\alpha_{Y_2})^{-1} \circ G_2(g) = \\ = G_2(g) \circ G_2(\alpha_{Y_1}) \circ \tau_{X_1} \circ G_2(\alpha_{Y_1})^{-1} = G_2(g) \circ \sigma_{Y_1} \ .\end{aligned}$$

So $\sigma \in \mathrm{Aut}_{\mathbf{C}}(G_2)$. Moreover, for any $X \in \mathrm{Ob}(\mathbf{C}_1)$ we can choose $X_{G_1(X)} = X$ and $\alpha_{G_1(X)} = \mathrm{id}_{G_1(X)}$. Then

$$\begin{aligned}\sigma_{G_1(X)} = G_2(\alpha_{G_1(X)}) \circ \tau_X \circ G_2(\alpha_{G_1(X)})^{-1} = \\ = G_2(\mathrm{id}_{G_1(X)}) \circ \tau_X \circ G_2(\mathrm{id}_{G_1(X)})^{-1} = \mathrm{id}_{(G_2 \circ G_1)(X)} \circ \tau_X \circ \mathrm{id}_{(G_2 \circ G_1)(X)} = \tau_X \ .\end{aligned}$$

So $\varphi(\sigma) = (\sigma_{G_1(X)})_{X \in \mathrm{Ob}(\mathbf{C}_1)} = (\tau_X)_{X \in \mathrm{Ob}(\mathbf{C}_1)} = \tau$. This shows that φ is surjective. It remains to prove that φ is open. Since we already know that φ is bijective, it is enough to check that the elements of the subbase of $\mathrm{Aut}(G_2)$ are sent to open subsets of $\mathrm{Aut}(G_2 \circ G_1)$. Let Y_0 be an object of $\mathbf{C}_2$ and $\tau \in \mathrm{Aut}_{\mathbf{C}_3}(G_2(Y_0))$. Since G_1 is essentially surjective, there exists an object X_0 of $\mathbf{C}_1$ such that $Y_0 \cong G_1(X_0)$. Let $\alpha : G_1(X_0) \to Y_0$ be an isomorphism. Then $G_2(\alpha) : (G_2 \circ G_1)(X_0) \to G_2(Y_0)$ is an isomorphism in $\mathbf{C}_3$ and $\tau' := G_2(\alpha)^{-1} \circ \tau \circ G_2(\alpha) \in \mathrm{Aut}_{\mathbf{C}_3}((G_2 \circ G_1)(X_0))$. For any $\sigma = (\sigma_Y)_{Y \in \mathrm{Ob}(\mathbf{C}_2)} \in \mathrm{Aut}(G_2)$, we have that $\sigma_{Y_0} = G_2(\alpha) \circ \sigma_{G_1(X_0)} \circ G_2(\alpha)^{-1}$, by definition of automorphism of a functor. Then

$$\begin{aligned}&g_{Y_0}^{-1}(\{\tau\}) = \\ &= \{\sigma = (\sigma_Y)_{Y \in \mathrm{Ob}(\mathbf{C}_2)} \in \mathrm{Aut}(G_2) \mid G_2(\alpha) \circ \sigma_{G_1(X_0)} \circ G_2(\alpha)^{-1} = \sigma_{Y_0} = \tau\} = \\ &= \{\sigma = (\sigma_Y)_{Y \in \mathrm{Ob}(\mathbf{C}_2)} \in \mathrm{Aut}(G_2) \mid \sigma_{G_1(X_0)} = G_2(\alpha)^{-1} \circ \tau \circ G_2(\alpha) = \tau'\} = \\ &= g_{G_1(X_0)}^{-1}(\{\tau'\}) = (f_{X_0} \circ \varphi)^{-1}(\{\tau'\}) = \varphi^{-1}(f_{X_0}^{-1}(\{\tau'\})) \ .\end{aligned}$$

So, since φ is bijective, we have that $\varphi(g_{Y_0}^{-1}(\{\tau\})) = f_{X_0}^{-1}(\{\tau'\})$, which is open by the definition of the topology on $\mathrm{Aut}(G_2 \circ G_1)$. Then φ is open. Hence φ is both a group isomorphism and a homeomorphism. □

Lemma 1.4.25. *Let $(\pi_k)_{k \in K}$ be a family of finite groups (with K an arbitrary index set) and consider on each π_k the discrete topology. Then the product $\prod_{k \in K} \pi_k$, with the product topology, is a profinite group.*

Proof. Let I be the set of finite subsets of K. If A, B are two finite subsets of K, we say that $A \geq B$ if and only if $A \supseteq B$. This is clearly an order relation. Moreover, I with this order relation is a directed partially ordered set. Indeed, if $A, B \in I$ then $A \cup B$ is also a finite subset of K, i.e. $A \cup B \in I$, and we have $A \cup B \geq A$ and $A \cup B \geq B$. We define now a projective system of finite groups. For any $A \in I$, define $\pi_A := \prod_{k \in A} \pi_k$. Since each π_k is finite and A is finite, we have that π_A is a finite group. We consider on π_A the product topology, which coincides with the discrete one. If $A, B \in I$ and $A \geq B$, define

$$f_{AB} : \pi_A = \prod_{k \in A} \pi_k \to \pi_B = \prod_{k \in B} \pi_k, \ (x_k)_{k \in A} \mapsto (x_k)_{k \in B} \ .$$

This is obviously a group homomorphism. Moreover, we have $f_{AA} = \mathrm{id}_{\pi_A}$ for any $A \in I$ and, if $A, B, C \in I$ are such that $A \geq B$ and $B \geq C$, $f_{AC} = f_{BC} \circ f_{AB}$. So $(\pi_A)_{A \in I}, (f_{AB} : \pi_A \to \pi_B)_{A,B \in I,\, A \geq B}$ is a projective system. Then we can consider the group $\pi = \varprojlim_{A \in I} \pi_A$. We claim that $\prod_{k \in K} \pi_k \cong \pi$. For any $A \in I$, consider the group homomorphism $g_A : \prod_{k \in K} \pi_k \to \pi_A = \prod_{k \in A} \pi_k$, $(x_k)_{k \in K} \mapsto (x_k)_{k \in A}$. We have that g_A is also continuous because its components coincide with the projections, which are continuous by definition of product topology. Moreover, if $A, B \in I$ are such that $A \geq B$, we have

$$g_B(x) = (x_k)_{k \in B} = f_{AB}\left((x_k)_{k \in A}\right) = f_{AB}(g_A(x))$$

for any $x = (x_k)_{k \in K} \in \prod_{k \in K} \pi_k$, i.e. $g_B = f_{AB} \circ g_A$. Then, by the universal property of the projective limit, there exists a unique continuous group homomorphism $g : \prod_{k \in K} \pi_k \to \pi$ such that $f_A \circ g = g_A$ for any $A \in I$, where $f_A : \pi \to \pi_A$ is the canonical projection.
On the other hand, let $k \in K$. Then $\{k\} \in I$ and $\pi_{\{k\}} = \pi_k$. So we can define $h_k := f_{\{k\}} : \pi \to \pi_{\{k\}} = \pi_k$ (the canonical projection, which is a continuous group homomorphism by definition of the topology and of the group structure on the projective limit). Let $h : \pi \to \prod_{k \in K} \pi_k$ be the map with k-th component h_k for any $k \in K$, i.e. $p_k \circ h = h_k$, where p_k is the canonical projection. Then h is a continuous group homomorphism, because each component is a continuous group homomorphism. We have that

$$p_k \circ (h \circ g) = h_k \circ g = f_{\{k\}} \circ g = g_{\{k\}} = p_k = p_k \circ \mathrm{id}_{\prod_{k \in K} \pi_k}$$

for any $k \in K$. So $h \circ g = \mathrm{id}_{\prod_{k \in K} \pi_k}$. Conversely, if $A \in I$, the k-th component of $f_A \circ (g \circ h) = g_A \circ h$ is $p_k \circ h = h_k = f_{\{k\}}$ for any $k \in A$ and so $f_A \circ (g \circ h) = f_A = f_A \circ \mathrm{id}_\pi$. Since this holds for any $A \in I$, we must have $g \circ h = \mathrm{id}_\pi$. This shows that $\prod_{k \in K} \pi_k \cong \pi$ (as topological groups) and hence $\prod_{k \in K} \pi_k$ is a profinite group. □

Lemma 1.4.26. *A closed subgroup of a profinite group is a profinite group.*

Proof. Let π be an arbitrary profinite group (unlike in the rest of this section, here π does not denote the projective limit of the projective system introduced in the proposition 1.3.14(3)). Then there exists a projective system of finite groups $I, (\pi_i)_{i \in I}, (f_{ij} : \pi_i \to \pi_j)_{i,j \in I,\, i \geq j}$ such that $\pi \cong \varprojlim_{i \in I} \pi_i$. We can assume without loss of generality that $\pi = \varprojlim_{i \in I} \pi_i$. Let π' be a closed subgroup of π. For any $i \in I$, let $f_i : \pi \to \pi_i$ be the canonical projection, which is a continuous group homomorphism by definition of the topology and of the group structure on the projective limit. Define $\pi'_i := f_i(\pi') \leq \pi_i$. Then π'_i is a finite group. Moreover, for any $i, j \in I$ such that $i \geq j$ we have that $f_{ij}(\pi'_i) = f_{ij}(f_i(\pi')) = (f_{ij} \circ f_i)(\pi') = f_j(\pi') = \pi'_j$ (the definition of projective limit implies that $f_{ij} \circ f_i = f_j$). So we can restrict f_{ij} to π'_i and get a (surjective) group homomorphism $f'_{ij} = (f_{ij})_{|_{\pi'_i}} : \pi'_i \to \pi'_j$. It is clear that $(\pi'_i)_{i \in I}, (f'_{ij} : \pi'_i \to \pi'_j)_{i,j \in I,\, i \geq j}$ is a projective system. We will show that $\pi' = \varprojlim_{i \in I} \pi'_i$. First of all, we prove that $\pi' = \pi \cap \prod_{i \in I} \pi'_i$ (as subsets of $\prod_{i \in I} \pi_i$). If $\sigma = (\sigma_i)_{i \in I} \in \pi'$, then for any $i \in I$ we have $\sigma_i = f_i(\sigma) \in f_i(\pi') = \pi'_i$. So $\sigma \in \prod_{i \in I} \pi'_i$. This shows that $\pi' \subseteq \prod_{i \in I} \pi'_i$. But we have also that $\pi' \subseteq \pi$, by assumption. So

$\pi' \subseteq \pi \cap \prod_{i\in I} \pi'_i$.
Conversely, let $\sigma = (\sigma_i)_{i\in I} \in \pi \cap \prod_{i\in I} \pi'_i$. In particular, $\sigma \in \pi$. We want to show that $\sigma \in \overline{\pi'}$ (topological closure). Let U be a neighbourhood of σ in π. By definition of the topology on the projective limit, a local base for π at σ is given by

$$\left\{ U_{i_1\dots i_n} := \bigcap_{k=1}^{n} f_{i_k}^{-1}(\{\sigma_{i_k}\}) \;\middle|\; n \in \mathbb{N},\ i_1,\dots,i_n \in I \right\}.$$

Then there exist $n \in \mathbb{N}$, $i_1, \dots, i_n \in I$ such that $U_{i_1\dots i_n} \subseteq U$. By definition of projective system, I is directed. So there exists $j \in I$ such that $j \geq i_k$ for any $k = 1,\dots,n$. We claim that $U_j \subseteq U_{i_1\dots i_n}$. Let $\tau = (\tau_i)_{i\in I} \in U_j = f_j^{-1}(\{\sigma_j\})$. Then $\tau_j = f_j(\tau) = \sigma_j$. Since $\sigma, \tau \in \pi = \varprojlim_{i\in I} \pi_i$, we have that $f_{i_k}(\tau) = \tau_{i_k} = f_{ji_k}(\tau_j) = f_{ji_k}(\sigma_j) = \sigma_{i_k}$ for any $k = 1,\dots,n$ (definition of projective limit). Then $\tau \in f_{i_k}^{-1}(\{\sigma_{i_k}\})$ for any $k = 1,\dots,n$ and this shows that $\tau \in \bigcap_{k=1}^{n} f_{i_k}^{-1}(\{\sigma_{i_k}\}) = U_{i_1\dots i_n}$. So $U_j \subseteq U_{i_1\dots i_n} \subseteq U$. Since $\sigma \in \prod_{i\in I} \pi'_i$, we have that $\sigma_j \in \pi'_j = f_j(\pi')$. Then there exists $\tau \in \pi'$ such that $\sigma_j = f_j(\tau)$, i.e. $\tau \in f_j^{-1}(\{\sigma_j\}) = U_j$. So $\tau \in \pi' \cap U_j$, which shows that $\pi' \cap U_j \neq \emptyset$. Then we have also that $\pi' \cap U \neq \emptyset$, because $\pi' \cap U_j \subseteq \pi' \cap U$. Since this holds for any neighbourhood of σ in π, we have that $\sigma \in \overline{\pi'}$. But π' is closed by assumption, so $\overline{\pi'} = \pi'$ and $\sigma \in \pi'$. This proves that $\pi' = \pi \cap \prod_{i\in I} \pi'_i$.
We have that $\varprojlim_{i\in I} \pi'_i$ is a subgroup of $\prod_{i\in I} \pi'_i \leq \prod_{i\in I} \pi_i$, so we can see $\varprojlim_{i\in I} \pi'_i$ as a subgroup of $\prod_{i\in I} \pi_i$ (with the subspace topology). Let $\sigma = (\sigma_i)_{i\in I} \in \varprojlim_{i\in I} \pi'_i$. Then, by definition of projective limit, we have that $\sigma_j = f'_{ij}(\sigma_i) = f_{ij}(\sigma_i)$ for any $i, j \in I$ with $i \geq j$. So $\sigma \in \varprojlim_{j\in J} \pi_j = \pi$. Then we have that $\sigma \in \pi \cap \prod_{i\in I} \pi'_i$. This shows that $\varprojlim_{i\in I} \pi'_i \subseteq \pi \cap \prod_{i\in I} \pi'_i$. Conversely, let $\sigma = (\sigma_i)_{i\in I} \in \pi \cap \prod_{i\in I} \pi'_i$. Then for any $i \in I$ we have that $\sigma_i \in \pi'_i$. Moreover, $\sigma \in \pi = \varprojlim_{i\in I} \pi_i$ and so $\sigma_j = f_{ij}(\sigma_i) = f'_{ij}(\sigma_i)$ for any $i, j \in I$ such that $i \geq j$. This shows that $\sigma \in \varprojlim_{i\in I} \pi'_i$. Hence $\pi' = \pi \cap \prod_{i\in I} \pi'_i = \varprojlim_{i\in I} \pi'_i$ is a profinite group. □

Lemma 1.4.27. *The automorphism group of the fundamental functor F is a profinite group.*

Proof. Since $\mathbf{C}$ is essentially small, there exist a small category $\mathbf{C}'$ and an equivalence of categories $G : \mathbf{C}' \to \mathbf{C}$. Define $F' = F \circ G : \mathbf{C}' \to \mathbf{sets}$. By lemma 1.4.24, we have that $\mathrm{Aut}(F) \cong \mathrm{Aut}(F')$ as topological groups. So it is enough to prove that $\mathrm{Aut}(F')$ is profinite. We can see $\mathrm{Aut}(F')$ as a subgroup of $\prod_{X\in \mathrm{Ob}(\mathbf{C}')} \mathrm{S}_{F'(X)}$, where $\mathrm{S}_{F'(X)}$ is the symmetric group on $F'(X)$ (which is a finite group because $F'(X)$ is a finite set). Notice that it makes sense to consider this product because $\mathrm{Ob}(\mathbf{C}')$ is a set. Moreover, the topology on $\mathrm{Aut}(F')$, defined as in remark 1.4.23(3), coincides with the subspace topology of the product, if we consider the discrete topology on $\mathrm{S}_{F'(X)}$ for any X. By lemma 1.4.25, we have that $\prod_{X\in \mathrm{Ob}(\mathbf{C}')} \mathrm{S}_{F'(X)}$, with the product topology, is a profinite group, because it is a product of finite groups. We prove now that $\mathrm{Aut}(F')$ is closed in $\prod_{X\in \mathrm{Ob}(\mathbf{C}')} \mathrm{S}_{F'(X)}$. For any morphism $f : Y \to Z$ in $\mathbf{C}'$, define

$$C_f := \left\{ (\sigma_X)_{X\in \mathrm{Ob}(\mathbf{C}')} \in \prod_{X\in \mathrm{Ob}(\mathbf{C}')} \mathrm{S}_{F'(X)} \;\middle|\; \sigma_Z \circ F'(f) = F'(f) \circ \sigma_Y \right\}.$$

Then we have that $\mathrm{Aut}(F') = \bigcap_{Y,Z\in \mathrm{Ob}(\mathbf{C}'),\, f:Y\to Z} C_f$. Let $f : Y \to Z$ be a morphism in $\mathbf{C}'$. Define the map

$$p_{ZY} : \prod_{X\in \mathrm{Ob}(\mathbf{C}')} \mathrm{S}_{F'(X)} \to \mathrm{S}_{F'(Z)} \times \mathrm{S}_{F'(Y)},\ (\sigma_X)_{X\in \mathrm{Ob}(\mathbf{C}')} \mapsto (\sigma_Z, \sigma_Y)\ .$$

Then, if we consider on $\mathrm{S}_{F'(Z)} \times \mathrm{S}_{F'(Y)}$ the product topology (which coincides with the discrete one), p_{ZY} is continuous, because its components are the canonical projections on $\mathrm{S}_{F'(Z)}$ and $\mathrm{S}_{F'(Y)}$, which are continuous by definition of the product topology on $\prod_{X\in \mathrm{Ob}(\mathbf{C}')} \mathrm{S}_{F'(X)}$. Consider now the set

$$A_f := \{(\sigma_1, \sigma_2) \in \mathrm{S}_{F'(Z)} \times \mathrm{S}_{F'(Y)} \mid \sigma_1 \circ F'(f) = F'(f) \circ \sigma_2\} \subseteq \mathrm{S}_{F'(Z)} \times \mathrm{S}_{F'(Y)}\ .$$

We have that $C_f = p_{ZY}^{-1}(A_f)$ (see the definitions). But A_f is closed in $\mathrm{S}_{F'(Z)} \times \mathrm{S}_{F'(Y)}$, which has the discrete topology. So C_f is closed in $\prod_{X\in \mathrm{Ob}(\mathbf{C}')} \mathrm{S}_{F'(X)}$. Then $\mathrm{Aut}(F')$ is closed in $\prod_{X\in \mathrm{Ob}(\mathbf{C}')} \mathrm{S}_{F'(X)}$, because it is the intersection of closed subsets. Hence $\mathrm{Aut}(F')$ is a profinite group, by lemma 1.4.26. □

Remark 1.4.28. In the proof of lemma 1.4.27, we did not use the axioms of Galois categories. We used only the fact that $\mathbf{C}$ is essentially small. So the result is true for any essentially small category with a functor to the category of finite sets.

Lemma 1.4.29. *For any object Y of $\mathbf{C}$, we have a continuos action of $\mathrm{Aut}(F)$ on $F(Y)$, defined by $\sigma y = \sigma_Y(y)$ for any $\sigma = (\sigma_X)_{X\in \mathrm{Ob}(\mathbf{C})} \in \mathrm{Aut}(F)$, $y \in F(Y)$. We denote by $H'(Y)$ the set $F(Y)$ equipped with this action. Then $H'(Y)$ is an object of $\mathrm{Aut}(F)$-**sets** (recall that $F(Y)$ is a finite set). Moreover, if Y, Z are objects of $\mathbf{C}$ with a morphism $h : Y \to Z$, then $F(h)$ is a morphism of $\mathrm{Aut}(F)$-sets. If we set $H'(f) = F(f)$, then $H' : \mathbf{C} \to \mathrm{Aut}(F)$-**sets** is a functor.*

Proof. Let Y be an object of $\mathbf{C}$. Since $1_{\mathrm{Aut}(F)} = (\mathrm{id}_{F(X)})_{X\in \mathrm{Ob}(\mathbf{C})}$, we have that $1_{\mathrm{Aut}(F)} y = \mathrm{id}_{F(Y)}(y) = y$, for any $y \in Y$. Moreover, let $\sigma = (\sigma_X)_{X\in \mathrm{Ob}(\mathbf{C})}, \tau = (\tau_X)_{X\in \mathrm{Ob}(\mathbf{C})} \in \mathrm{Aut}(F)$. Then $\sigma\tau = (\sigma_X \circ \tau_X)_{X\in \mathrm{Ob}(\mathbf{C})}$ and so $(\sigma\tau)y = (\sigma_Y \circ \tau_Y)(y) = \sigma_Y(\tau_Y(y)) = \sigma(\tau_Y(y)) = \sigma(\tau y)$. So we have indeed defined a group action. We have to prove that this action is continuous. Let $y \in F(Y)$. Then

$$\begin{aligned}\mathrm{Stab}_{\mathrm{Aut}(F)}(y) = \{\sigma = (\sigma_X)_{X\in \mathrm{Ob}(\mathbf{C})} \in \mathrm{Aut}(F) \mid y = \sigma y = \sigma_Y(y)\} = \\ = f_Y^{-1}(\mathrm{Stab}_{\mathrm{S}_{F(Y)}}(y))\ ,\end{aligned}$$

where $f_Y : \mathrm{Aut}(F) \to \mathrm{S}_{F(Y)}$, $\sigma = (\sigma_X)_{X\in \mathrm{Ob}(\mathbf{C})} \mapsto \sigma_Y$ is continuous by definition of the topology on $\mathrm{Aut}(F)$ (remark 1.4.23(3)), if we consider the discrete topology on $\mathrm{S}_{F(Y)}$. Then, since $\mathrm{Stab}_{\mathrm{S}_{F(Y)}}$ is open in $\mathrm{S}_{F(Y)}$, we have that $\mathrm{Stab}_{\mathrm{Aut}(F)}(y)$ is open in $\mathrm{Aut}(F)$. So the action is continuous by lemma 1.1.14.
Let Y, Z be objects of $\mathbf{C}$ and $h : Y \to Z$ a morphism. Let $y \in Y$ and $\sigma = (\sigma_X)_{X\in \mathrm{Ob}(\mathbf{C})} \in \mathrm{Aut}(F)$. By definition of automorphism of a functor, we have that $\sigma_Z \circ F(h) = F(h) \circ \sigma_Y$. Then we have that

$$F(h)(\sigma y) = F(h)(\sigma_Y(y)) = \sigma_Z(F(h)(y)) = \sigma F(h)(y)\ .$$

So $F(h)$ is a morphism of $\mathrm{Aut}(F)$-sets.
It remains to prove that H' is a functor. This follows immediately from the fact that F is a functor. Indeed, $H'(\mathrm{id}_Y) = F(\mathrm{id}_Y) = \mathrm{id}_{F(Y)} = \mathrm{id}_{H'(Y)}$ for any object Y of $\mathbf{C}$ and $H'(h_2 \circ h_1) = F(h_2 \circ h_1) = F(h_2) \circ F(h_1) = H'(h_1) \circ H'(h_2)$ for any $h_1 : Y \to Z$, $h_2 : Z \to W$ morphisms in $\mathbf{C}$. □

Remark 1.4.30. If H' is the functor defined in 1.4.29, then $\mathrm{for}_{\mathrm{Aut}(F)} \circ H' = F$, where $\mathrm{for}_{\mathrm{Aut}(F)} : \mathrm{Aut}(F)\textbf{-sets} \to \textbf{sets}$ is the forgetful functor.

Now we want to prove that the functor H' defined in 1.4.29 is an equivalence of categories. We need some lemmas.

Lemma 1.4.31. *The intersection of all open normal subgroups of a profinite group is trivial.*

Proof. Let π be an arbitrary profinite group (unlike in the rest of this section, here π does not denote the projective limit of the projective system introduced in the proposition 1.3.14(3)). Then there exists a projective system of finite groups $I, (\pi_i)_{i \in I}, (f_{ij} : \pi_i \to \pi_j)_{i,j \in I, i \geq j}$ such that $\pi \cong \varprojlim_{i \in I} \pi_i$. We can assume without loss of generality that $\pi = \varprojlim_{i \in I} \pi_i$. Let $x \in \bigcap_{\pi' \trianglelefteq \pi, \, \pi' \text{ open}} \pi'$. We claim that $1 \in \overline{\{x\}}$ (topological closure). Let U be a neighbourhood of 1. By definition of the topology on the projective limit, a local base for π at 1 is given by

$$\left\{ U_{j_1 \dots j_n} := \bigcap_{k=1}^{n} p_{j_k}^{-1}(\{1_{j_k}\}) = \bigcap_{k=1}^{n} \mathrm{Ker}(p_{j_k}) \;\middle|\; n \in \mathbb{N},\ j_1, \dots, j_n \in I \right\} ,$$

where $p_j : \pi = \varprojlim_{i \in I} \pi_i \to \pi_j$ is the canonical projection (which is a continuous group homomorphism) for any $j \in I$. So there exist $n \in \mathbb{N}$, $j_1, \dots, j_n \in I$ such that $U_{j_1 \dots j_n} \subseteq U$. For any $k = 1, \dots, n$, we have that $\mathrm{Ker}(p_{j_k})$ is an open normal subgroup of π. So $x \in \mathrm{Ker}(p_{j_k})$. Then $x \in \bigcap_{k=1}^{n} \mathrm{Ker}(p_{j_k}) = U_{j_1 \dots j_n} \subseteq U$. This proves that $U \cap \{x\} \neq \emptyset$. Since this holds for any U, we have that $1 \in \overline{\{x\}}$. But π is Hausdorff, by remark 1.1.10. In particular, points are closed. So $\overline{\{x\}} = \{x\}$. Hence $x = 1$. □

Lemma 1.4.32. *In this lemma, we do not use the notation introduced in proposition 1.3.14 and we denote by π an arbitrary profinite group. We denote by* $\mathrm{for} : \pi\textbf{-sets} \to \textbf{sets}$ *the forgetful functor. Since* π**-sets** *is a Galois category with fundamental functor* for, *we can define a functor* $H' : \pi\textbf{-sets} \to \mathrm{Aut}(\mathrm{for})\textbf{-sets}$ *as in lemma 1.4.29. For any open subgroup π' of π, we see π/π' as a π-set with action of π given by left multiplication, as in lemma 1.4.9.*

(1) The map

$$\varphi : \mathrm{Aut}(\mathrm{for}) \to \prod_{\substack{\pi' \trianglelefteq \pi \\ \pi' \text{ open}}} \mathrm{S}_{\pi/\pi'},\ (\sigma_X)_{X \in \mathrm{Ob}(\pi\textbf{-sets})} \mapsto (\sigma_{\pi/\pi'})_{\pi' \trianglelefteq \pi, \, \pi' \text{ open}}$$

is an injective group homomorphism.

(2) *Let π' be an open normal subgroup of π. The map*

$$\psi_{\pi'} : \pi/\pi' \to \mathrm{Aut}_{\pi\textbf{-sets}}(\pi/\pi'),\ \tau\pi' \mapsto \big(\tau'\pi' \mapsto (\tau'\tau^{-1})\pi'\big)$$

is an isomorphism of groups. Moreover, if $f : \pi/\pi' \to \pi/\pi'$ is a map of sets such that $f \circ \sigma = \sigma \circ f$ for any $\sigma \in \mathrm{Aut}_{\pi\textbf{-sets}}(\pi/\pi')$, then there exists a unique $\tau\pi' \in \pi/\pi'$ such that $f = f_{\tau\pi'}$, where $f_{\tau\pi'}$ is defined by $f_{\tau\pi'}(\tau'\pi') = (\tau\tau')\pi'$ for any $\tau'\pi' \in \pi/\pi'$ (it is immediate to check that $f_{\tau\pi'}$ is well defined for any $\tau\pi' \in \pi/\pi'$, using the fact that π' is normal).

(3) *We have that* $\mathrm{Aut}(\mathrm{for}) \cong \pi$ *as profinite groups and H' coincides with the functor induced by this isomorphism.*

Proof. (1) The fact that φ is a group homomorphism follows from the definition of the group structure on Aut(for). Let $\sigma = (\sigma_X)_{X \in \mathrm{Ob}(\pi\textbf{-sets})} \in \mathrm{Ker}(\varphi)$. Then

$$(\sigma_{\pi/\pi'})_{\pi' \trianglelefteq \pi,\, \pi' \text{ open}} = \varphi(\sigma) = (\mathrm{id}_{\pi/\pi'})_{\pi' \trianglelefteq \pi,\, \pi' \text{ open}}\ ,$$

i.e. $\sigma_{\pi/\pi'} = \mathrm{id}_{\pi/\pi'}$ for any open normal subgroup π' of π. Let X be an object of π**-sets**. We can write X as the disjoint union of its orbits: $X = \coprod_{i=1}^n X_i$ ($n \in \mathbb{N}$), such that the action of π on X_i is transitive for any $i = 1, \dots, n$. Let $x \in X$. Then there exists a unique $i \in \{1, \dots, n\}$ such that $x \in X_i$. Denote by $q_i : X_i \to X$ the canonical inclusion, which is a morphism of π-sets. Then, since σ is an automorphism of for, we have that

$$\sigma_X \circ q_i = \sigma_X \circ \mathrm{for}(q_i) = \mathrm{for}(q_i) \circ \sigma_{X_i} = q_i \circ \sigma_{X_i}\ .$$

So $\sigma_X(x) = \sigma_X(q_i(x)) = q_i(\sigma_{X_i}(x)) = \sigma_{X_i}(x)$. By lemma 1.4.9 there exists an open subgroup $\pi_i \leq \pi$ such that X_i is isomorphic to π/π_i as a π-set. Let $\alpha_i : X_i \to \pi/\pi_i$ be an isomorphism of π-sets. Since σ is an automorphism of for, we have that $\sigma_{X_i} = \mathrm{for}(\alpha_i)^{-1} \circ \sigma_{\pi/\pi_i} \circ \mathrm{for}(\alpha_i) = \alpha_i^{-1} \circ \sigma_{\pi/\pi_i} \circ \alpha_i$. Moreover, let π_i' be the normal core of π_i, i.e. $\pi_i' := \bigcap_{\tau \in \pi} \tau\pi_i\tau^{-1} \trianglelefteq \pi$. Since π_i is open, it has finite index in π, by lemma 1.1.11. Notice that, if $\tau_1\pi_i = \tau_2\pi_i$ with $\tau_1, \tau_2 \in \pi$, then $\tau_1\pi_i\tau_1^{-1} = \tau_2\pi_i\tau_2^{-1}$. So the set $\{\tau\pi_i\tau^{-1} \mid \tau \in \pi\}$ is finite. Since π is a topological group, conjugation by τ is a homeomorphism for any $\tau \in \pi$ and so $\tau\pi_i\tau^{-1}$ is open, because π_i is open. Then π_i' is open in π, because it is a finite intersection of open subsets. So π_i' is an open normal subgroup of π, which implies that $\sigma_{\pi/\pi_i'} = \mathrm{id}_{\pi/\pi_i'}$. Consider the map $\beta_i : \pi/\pi_i' \to \pi/\pi_i,\ \tau\pi_i' \mapsto \tau\pi_i$. This map is well defined, because $\pi_i' \subseteq \pi_i$. Moreover, β_i is clearly a morphism of π-sets, by definition of the action on π on π/π_i' and on π/π_i. Since σ is an automorphism of for, we have that

$$\sigma_{\pi/\pi_i} \circ \beta_i = \sigma_{\pi/\pi_i} \circ \mathrm{for}(\beta_i) = \mathrm{for}(\beta_i) \circ \sigma_{\pi/\pi_i'} = \beta_i \circ \mathrm{id}_{\pi/\pi_i'} = \beta_i = \mathrm{id}_{\pi/\pi_i} \circ \beta_i\ .$$

But β_i is clearly surjective and so an epimorphism of sets (see example 1.1.3(6)). Then we must have $\sigma_{\pi/\pi_i} = \mathrm{id}_{\pi/\pi_i}$. So $\sigma_{X_i} = \alpha_i^{-1} \circ \sigma_{\pi/\pi_i} \circ \alpha_i = \alpha_i^{-1} \circ \alpha_i = \mathrm{id}_{X_i}$ and $\sigma_X(x) = \sigma_{X_i}(x) = x$. Since this holds for any $x \in X$, we have that $\sigma_X = \mathrm{id}_X$. Then $\sigma = (\mathrm{id}_X)_{X \in \mathrm{Ob}(\pi\textbf{-sets})} = 1_{\mathrm{Aut(for)}}$. Hence φ is injective.

(2) First of all, we check that $\psi_{\pi'}$ is well defined. Consider $\tau\pi' \in \pi/\pi'$. If $\tau'\pi' = \tau''\pi'$, with $\tau', \tau'' \in \pi$, then $(\tau'')^{-1}\tau' \in \pi'$ and so

$$\left(\tau''\tau^{-1}\right)^{-1}\left(\tau'\tau^{-1}\right) = \tau\left((\tau'')^{-1}\tau'\right)\tau^{-1} \in \pi' ,$$

because π' is normal. So $(\tau'\tau^{-1})\pi' = (\tau''\tau^{-1})\pi'$. This shows that the map $\pi/\pi' \to \pi/\pi'$, $\tau'\pi' \mapsto (\tau'\tau^{-1})\pi'$ is well defined. Moreover, it is a morphism of π-sets. Indeed, if $\sigma \in \pi$, we have that $((\sigma\tau')\tau^{-1})\pi' = (\sigma(\tau'\tau^{-1}))\pi' = \sigma((\tau'\tau^{-1})\pi')$. It remains to check that this map does not depend on the choice of τ. If $\tau_1\pi' = \tau_2\pi'$, with $\tau_1, \tau_2 \in \pi$, then $\tau_2^{-1}\tau_1 \in \pi'$. So, for any $\tau'\pi' \in \pi/\pi'$, we have that

$$\left(\tau'\tau_1^{-1}\right)^{-1}\left(\tau'\tau_2^{-1}\right) = \tau_1(\tau')^{-1}\tau'\tau_2^{-1} = \tau_1\tau_2^{-1} = \tau_1\left(\tau_2^{-1}\tau_1\right)\tau_1^{-1} \in \pi' ,$$

because π' is normal in π. Then $(\tau'\tau_1^{-1})\pi' = (\tau'\tau_2^{-1})\pi'$. So $\psi_{\pi'}$ is well defined. Let $\tau_1\pi', \tau_2\pi' \in \pi/\pi'$. For any $\tau'\pi' \in \pi/\pi'$, we have

$$\begin{aligned}\left(\psi_{\pi'}(\tau_1\pi') \circ \psi_{\pi'}(\tau_2\pi')\right)(\tau'\pi') = \psi'_{\pi}(\tau_1\pi')\left(\left(\tau'\tau_2^{-1}\right)\pi'\right) = \\ = \left(\left(\tau'\tau_2^{-1}\right)\tau_1^{-1}\right)\pi' = \left(\tau'(\tau_1\tau_2)^{-1}\right)\pi' = \psi_{\pi'}((\tau_1\tau_2)\pi')(\tau'\pi') .\end{aligned}$$

So $\psi_{\pi'}(\tau_1\pi') \circ \psi_{\pi'}(\tau_2\pi') = \psi_{\pi'}((\tau_1\tau_2)\pi') = \psi_{\pi'}((\tau_1\pi')(\tau_2\pi'))$, which shows that $\psi_{\pi'}$ is a group homomorphism. Let $\tau\pi' \in \mathrm{Ker}(\psi_{\pi'})$, i.e. $\psi_{\pi'}(\tau\pi') = \mathrm{id}_{\pi/\pi'}$. Then $\tau^{-1}\pi' = \psi_{\pi'}(\tau\pi')(\pi') = \mathrm{id}_{\pi/\pi'}(\pi') = \pi'$, which means that $\tau^{-1} \in \pi'$. Since π' is a subgroup of π, we must have also $\tau = (\tau^{-1})^{-1} \in \pi'$ and so $\tau\pi' = \pi'$. This shows that $\psi_{\pi'}$ is injective. It remains to prove that it is surjective. Let $\sigma \in \mathrm{Aut}_{\pi\textbf{-sets}}(\pi/\pi')$. Since $\sigma(\pi') \in \pi/\pi'$, there exists $\tau \in \pi$ such that $\sigma(\pi') = \tau\pi'$. Let $\tau'\pi' \in \pi/\pi'$, with $\tau' \in \pi$. Then, since σ is a morphism of π-sets, we have that $\sigma(\tau'\pi') = \sigma(\tau'(\pi')) = \tau'(\sigma(\pi')) = \tau'(\tau\pi') = (\tau'\tau)\pi' = \psi_{\pi'}(\tau^{-1}\pi')(\tau'\pi')$. So $\sigma = \psi_{\pi'}(\tau^{-1}\pi')$. This proves surjectivity.
Let now $f : \pi/\pi' \to \pi/\pi'$ be a map such that $f \circ \sigma = \sigma \circ f$ for any $\sigma \in \mathrm{Aut}_{\pi\textbf{-sets}}(\pi/\pi')$. Since $f(\pi') \in \pi/\pi'$, there exists $\tau \in \pi$ such that $f(\pi') = \tau\pi'$. Let $\tau'\pi' \in \pi/\pi'$ and consider $\psi_{(\tau')^{-1}\pi'} \in \mathrm{Aut}_{\pi\textbf{-sets}}(\pi/\pi')$. Then $f \circ \psi_{(\tau')^{-1}\pi'} = \psi_{(\tau')^{-1}\pi'} \circ f$. We have that $\psi_{(\tau')^{-1}\pi'}(\pi') = \left((\tau')^{-1}\right)^{-1}\pi' = \tau'\pi'$ and so

$$\begin{aligned}f(\tau'\pi') = f\left(\psi_{(\tau')^{-1}\pi'}(\pi')\right) = \psi_{(\tau')^{-1}\pi'}(f(\pi')) = \\ = \psi_{(\tau')^{-1}\pi'}(\tau\pi') = (\tau\tau')\pi' = f_{\tau\pi'}(\tau'\pi') .\end{aligned}$$

Then $f = f_{\tau\pi'}$, as we wanted. If $\widetilde{\tau}\pi' \in \pi/\pi'$ is such that $f = f_{\widetilde{\tau}\pi'}$, then $\widetilde{\tau}\pi' = f_{\widetilde{\tau}\pi'}(\pi') = f(\pi') = \tau\pi'$. So we have uniqueness.

(3) For any $\tau \in \pi$ and any finite π-set X, define $\sigma_{X,\tau} : X \to X$, $x \mapsto \tau x$. By definition of group action, we have that $\sigma_{X,\tau^{-1}}$ is the inverse of $\sigma_{X,\tau}$, so $\sigma_{X,\tau}$ is bijective, i.e. $\sigma_{X,\tau} \in \mathrm{S}_X = \mathrm{S}_{\mathrm{for}(X)}$. Let X, Y be two finite π-sets, with a morphism of π-sets $h : X \to Y$. By definition of morphism of π-sets, we have that

$$(h \circ \sigma_{X,\tau})(x) = h(\tau x) = \tau h(x) = (\sigma_{Y,\tau} \circ h)(x) ,$$

for any $x \in X$. So $\mathrm{for}(h) \circ \sigma_{X,\tau} = h \circ \sigma_{X,\tau} = \sigma_{Y,\tau} \circ h = \sigma_{Y,\tau} \circ \mathrm{for}(h)$. This proves that $\sigma_\tau := (\sigma_{X,\tau})_{X \in \mathrm{Ob}(\pi\textbf{-sets})}$ is an automorphism of the functor for. Consider now the map

$$\Phi : \pi \to \mathrm{Aut}(\mathrm{for}),\ \tau \mapsto \sigma_\tau\ .$$

We claim that Φ is an isomorphism of topological groups. Let $\tau_1, \tau_2 \in \pi$ and let X be a finite π-set. By definition of group action, we have that

$$\sigma_{X,\tau_1\tau_2}(x) = (\tau_1\tau_2)x = \tau_1(\tau_2 x) = \\ = \sigma_{X,\tau_1}(\tau_2 x) = \sigma_{X,\tau_1}(\sigma_{X,\tau_2}(x)) = (\sigma_{X,\tau_1} \circ \sigma_{X,\tau_2})(x)\ ,$$

for any $x \in X$. So $\sigma_{X,\tau_1\tau_2} = \sigma_{X,\tau_1} \circ \sigma_{X,\tau_2}$. Then we have:

$$\Phi(\tau_1\tau_2) = \sigma_{\tau_1\tau_2} = (\sigma_{X,\tau_1\tau_2})_{X \in \mathrm{Ob}(\pi\textbf{-sets})} = (\sigma_{X,\tau_1} \circ \sigma_{X,\tau_2})_{X \in \mathrm{Ob}(\pi\textbf{-sets})} = \\ = (\sigma_{X,\tau_1})_{X \in \mathrm{Ob}(\pi\textbf{-sets})} \circ (\sigma_{X,\tau_2})_{X \in \mathrm{Ob}(\pi\textbf{-sets})} = \sigma_{\tau_1} \circ \sigma_{\tau_2} = \Phi(\tau_1)\Phi(\tau_2)\ .$$

So Φ is a group homomorphism. Let $\tau \in \mathrm{Ker}(\Phi)$, i.e.

$$(\sigma_{X,\tau})_{X \in \mathrm{Ob}(\pi\textbf{-sets})} = \sigma_\tau = \Phi(\tau) = 1_{\mathrm{Aut}(\mathrm{for})} = (\mathrm{id}_X)_{X \in \mathrm{Ob}(\pi\textbf{-sets})}\ .$$

Then $\sigma_{X,\tau} = \mathrm{id}_X$ for any finite π-set X. Let π' be an open normal subgroup of π. Then $\sigma_{\pi/\pi',\tau} = \mathrm{id}_{\pi/\pi'}$. So

$$\tau\pi' = \sigma_{\pi/\pi',\tau}(\pi') = \mathrm{id}_{\pi/\pi'}(\pi') = \pi'\ ,$$

which means that $\tau \in \pi'$. Then we have that $\tau \in \bigcap_{\pi' \trianglelefteq \pi,\, \pi' \text{ open}} \pi'$. By lemma 1.4.31, this implies $\tau = 1$. So Φ is injective. Let $\sigma = (\sigma_X)_{X \in \mathrm{Ob}(\pi\textbf{-sets})} \in \mathrm{Aut}(\mathrm{for})$. Let π' be an open normal subgroup of π. We have that $\sigma_{\pi/\pi'}$ is a (bijective) map from π/π' to π/π'. Let $\alpha \in \mathrm{Aut}_{\pi\textbf{-sets}}(\pi/\pi')$. By definition of automorphism of a functor, we have that $\sigma_{\pi/\pi'} \circ \alpha = \sigma_{\pi/\pi'} \circ \mathrm{for}(\alpha) = \mathrm{for}(\alpha) \circ \sigma_{\pi/\pi'} = \alpha \circ \sigma_{\pi/\pi'} \circ \alpha$. Then, by point (2), there exists $\tau_{\pi'}\pi' \in \pi/\pi'$ such that $\sigma_{\pi/\pi'} = f_{\tau_{\pi'}\pi'}$. We want now to find $\tau \in \pi$ such that $\tau_{\pi'}\pi' = \tau\pi'$ for any open normal subgroup π'. This means that $\tau \in \tau_{\pi'}\pi'$ for any open normal subgroup π'. So it is enough to show that $\bigcap_{\pi' \trianglelefteq \pi,\, \pi' \text{ open}}(\tau_{\pi'}\pi') \neq \emptyset$. For any normal open subgroup π', left multiplication by $\tau_{\pi'}$ is a homeomorphism, because π is a topological group. Moreover, by lemma 1.1.11, π' open implies π' closed. So $\tau_{\pi'}\pi'$ is closed. Since π is a profinite group, it is compact. Then, in order to prove that $\bigcap_{\pi' \trianglelefteq \pi,\, \pi' \text{ open}}(\tau_{\pi'}\pi') \neq \emptyset$, it is enough to show that $(\tau_{\pi'_1}\pi'_1) \cap \cdots \cap (\tau_{\pi'_n}\pi'_n) \neq \emptyset$ for any $n \in \mathbb{N}$, $\pi'_1, \ldots, \pi'_n$ open normal subgroups of π. Given such $\pi'_1, \ldots, \pi'_n$, define $\pi' := \pi'_1 \cap \cdots \cap \pi'_n$. Then π' is a normal subgroup of π and it is also open, because it is a finite intersection of open subsets. Fix $i \in \{1, \ldots, n\}$ and consider the map $\beta_i : \pi/\pi' \to \pi/\pi'_i$, $\tau\pi' \mapsto \tau\pi'_i$, which is well defined because $\pi' \subseteq \pi'_i$. It is immediate to check that β_i is a morphism of π-sets, by definition of the action of π on π/π' and on π/π'_i. Since σ is an automorphism of for, we have that

$$f_{\tau_{\pi'_i}\pi'_i} \circ \beta_i = \sigma_{\pi/\pi'_i} \circ \mathrm{for}(\beta_i) = \mathrm{for}(\beta_i) \circ \sigma_{\pi/\pi'} = \beta_i \circ f_{\tau_{\pi'}\pi'}\ .$$

So $\tau_{\pi_i'}\pi_i' = f_{\tau_{\pi_i'}\pi_i'}(\pi_i') = f_{\tau_{\pi_i'}\pi_i'}(\beta_i(\pi')) = \beta_i(f_{\tau_{\pi'}\pi'}(\pi')) = \beta_i(\tau_{\pi'}\pi') = \tau_{\pi'}\pi_i'$. This means that $\tau_{\pi'} \in \tau_{\pi_i'}\pi_i'$. So $\tau_{\pi'} \in (\tau_{\pi_1'}\pi_1') \cap \cdots \cap (\tau_{\pi_n'}\pi_n')$, which shows that $(\tau_{\pi_1'}\pi_1') \cap \cdots \cap (\tau_{\pi_n'}\pi_n') \neq \emptyset$, as we wanted. Then there exists $\tau \in \pi$ such that $\tau_{\pi'}\pi' = \tau\pi'$ for any open normal subgroup π'. So $\sigma_{\pi/\pi'} = f_{\tau_\pi'\pi'} = f_{\tau\pi'}$. From the definitions, it is clear that $f_{\tau\pi'} = \sigma_{\pi/\pi',\tau}$. So $\sigma_{\pi/\pi'} = \sigma_{\pi/\pi',\tau}$, for any open normal subgroup π' of π. Then

$$\varphi(\sigma) = (\sigma_{\pi/\pi'})_{\pi' \trianglelefteq \pi,\, \pi' \text{ open}} = (\sigma_{\pi/\pi',\tau})_{\pi' \trianglelefteq \pi,\, \pi' \text{ open}} = \varphi(\sigma_\tau)\ .$$

Since φ is injective by point (1), we must have $\sigma = \sigma_\tau = \Phi(\tau)$. So Φ is surjective. Then Φ is a group isomorphism. We prove now that Φ is continuous. Recall that a subbase of the topology on Aut(for) is given by

$$\left\{ f_Y^{-1}(\{\sigma\}) \;\middle|\; Y \in \mathrm{Ob}(\pi\textbf{-sets}),\ \sigma \in \mathrm{S}_{\mathrm{for}(Y)} = \mathrm{S}_Y \right\}\ .$$

where we defined $f_Y : \mathrm{Aut(for)} \to \mathrm{S}_{\mathrm{for}(Y)} = \mathrm{S}_Y,\ (\sigma_X)_{X \in \mathrm{Ob}(\pi\textbf{-sets})} \mapsto \sigma_Y$. Let Y be a finite π-set and $\sigma \in \mathrm{S}_Y$. We have to prove that $\Phi^{-1}(f_Y^{-1}(\{\sigma\})) = (f_Y \circ \Phi)^{-1}(\{\sigma\})$ is open in π. Notice that, for any $\tau \in \pi$, $(f_Y \circ \Phi)(\tau) = \sigma_{Y,\tau}$. Then

$$(f_Y \circ \Phi)^{-1}(\{\sigma\}) = \{\tau \in \pi \mid \sigma_{Y,\tau} = \sigma\}\ .$$

If $(f_Y \circ \Phi)^{-1}(\{\sigma\}) = \emptyset$, then it is clearly open. Otherwise, let $\tau_0 \in (f_Y \circ \Phi)^{-1}(\{\sigma\})$, i.e. $\sigma_{Y,\tau_0} = \sigma$. If $\tau \in (f_Y \circ \Phi)^{-1}(\{\sigma\})$, then $\sigma_{Y,\tau} = \sigma$ and so $\sigma_{Y,\tau_0^{-1}\tau} = \sigma_{Y,\tau_0}^{-1} \circ \sigma_{Y,\tau} = \sigma^{-1} \circ \sigma = \mathrm{id}_Y$. So $\tau_0^{-1}\tau \in (f_Y \circ \Phi)^{-1}(\{\mathrm{id}_Y\})$ and this shows that $(f_Y \circ \Phi)^{-1}(\{\sigma\}) \subseteq \tau_0(f_Y \circ \Phi)^{-1}(\{\mathrm{id}_Y\})$. Conversely, if $\tau \in (f_Y \circ \Phi)^{-1}(\{id_Y\})$, then $\sigma_{Y,\tau} = \mathrm{id}_Y$ and so $\sigma_{Y,\tau_0\tau} = \sigma_{Y,\tau_0} \circ \sigma_{Y,\tau} = \sigma \circ \mathrm{id}_Y = \sigma$, which means that $\tau_0\tau \in (f_Y \circ \Phi)^{-1}(\sigma)$. So $(f_Y \circ \Phi)^{-1}(\{\sigma\}) = \tau_0(f_Y \circ \Phi)^{-1}(\{\mathrm{id}_Y\})$. Since π is a topological group, multiplication by τ_0 is a homeomorphism. Then, in order to prove that $(f_Y \circ \Phi)^{-1}(\{\sigma\}) = \tau_0(f_Y \circ \Phi)^{-1}(\{\mathrm{id}_Y\})$ is open, it is enough to prove that $(f_Y \circ \Phi)^{-1}(\{\mathrm{id}_Y\})$ is open. We have that

$$\begin{aligned}(f_Y \circ \Phi)^{-1}(\{\mathrm{id}_Y\}) &= \{\tau \in \pi \mid \sigma_{Y,\tau} = \mathrm{id}_Y\} = \\ &= \{\tau \in \pi \mid \forall y \in Y \quad \tau y = \sigma_{Y,\tau}(y) = \mathrm{id}_Y(y) = y\}\ .\end{aligned}$$

This is the kernel of the action of π on Y, which is open by lemma 1.1.14, since Y is finite. So Φ is continuous.
Since π is a profinite group, it is compact by remark 1.1.10. By lemma 1.4.27, also Aut(for) is profinite. In particular, it is Hausdorff, by remark 1.1.10. If $C \subseteq \pi$ is closed, then it is compact (a closed subspace of a compact space is compact) and so $\Phi(C)$ is compact in Aut(for). But a compact subspace of a Hausdorff space is closed. Then $\Phi(C)$ is closed. So Φ is a closed map. We already know that it is bijective and continuous, so it is a homeomorphism. This proves that Φ is an isomorphism of topological groups. So $\pi \cong \mathrm{Aut(for)}$ as profinite groups.
The isomorphism Φ induces an action of Aut(for) on any π-set Y: $\sigma.y = \Phi^{-1}(\sigma)y$ for any $\sigma \in \mathrm{Aut(for)}$, $y \in Y$. It is immediate to check that this is a continuous group action and that any morphism of π-sets is a morphism

of Aut(for)-sets. So we have a functor $H'' : \pi\text{-}\mathbf{sets} \to \text{Aut(for)-}\mathbf{sets}$, with $H''(Y) = Y$ equipped with the action of Aut(for), for any object Y of π-**sets**, and $H''(f) = f$, for any morphism $f : Y_1 \to Y_2$ in π-**sets**. We claim that this functor coincides with H'. We have $H'(f) = f = H''(f)$ for any morphism f in π-**sets**. So we have to check only that $H'(Y) = H''(Y)$, i.e. the two actions of Aut(for) coincide, for any object Y of π-**sets**. Let Y be an object of π-**sets**. Let $\sigma = (\sigma_X)_{X\in \text{Ob}(\pi\text{-}\mathbf{sets})} \in \text{Aut(for)}$ and $y \in Y$. The action induced by Φ (functor H'') gives us $\sigma.y = \Phi^{-1}(\sigma)y$, while the action defined as in lemma 1.4.29 (functor H') gives us $\sigma y = \sigma_Y(y)$. Let $\tau := \Phi^{-1}(\sigma)$. Then $\sigma = \Phi(\tau) = (\sigma_{X,\tau})_{X\in \text{Ob}(\pi\text{-}\mathbf{sets})}$. In particular, $\sigma_Y = \sigma_{Y,\tau}$. So

$$\sigma y = \sigma_Y(y) = \sigma_{Y,\tau}(y) = \tau y = \Phi^{-1}(\sigma)y = \sigma.y\ .$$

□

Lemma 1.4.33. *Let $\mathbf{C}_1$, $\mathbf{C}_2$ be two categories, with $\mathbf{C}_1$ essentially small, and let $F_1, F_2 : \mathbf{C}_1 \to \mathbf{C}_2$ be two functors. If F_1 and F_2 are isomorphic, then* $\text{Aut}(F_1) \cong \text{Aut}(F_2)$ *as profinite groups and the isomorphism is canonically determined up to an inner automorphism of* $\text{Aut}(F_1)$.

Proof. Let $\alpha : F_1 \to F_2$ be an isomorphism of functors, i.e. for any object X of $\mathbf{C}_1$ we have an isomorphism $\alpha_X : F_1(X) \to F_2(X)$ in $\mathbf{C}_2$ and these isomorphisms are compatible with each other, i.e. the following diagram is commutative for any morphism $f : X \to Y$ in $\mathbf{C}_1$.

$$\begin{array}{ccc} F_1(X) & \xrightarrow{\alpha_X} & F_2(X) \\ {\scriptstyle F_1(f)}\downarrow & & \downarrow{\scriptstyle F_2(f)} \\ F_1(Y) & \xrightarrow{\alpha_Y} & F_2(Y) \end{array}$$

If $\sigma = (\sigma_X)_{X\in \text{Ob}(\mathbf{C}_1)} \in \text{Aut}(F_1)$, then for any X we have that $\alpha_X \circ \sigma_X \circ \alpha_X^{-1} : F_2(X) \to F_2(X)$ is an isomorphism, because it is a composition of isomorphisms. So $\alpha_X \circ \sigma_X \circ \alpha_X^{-1} \in \text{Aut}_{\mathbf{C}_2}(F_2(X))$. It is immediate to check that these isomorphisms are compatible with each other, so $(\alpha_X \circ \sigma_X \circ \alpha_X^{-1})_{X\in \text{Ob}(\mathbf{C}_1)}$ is an automorphism of F_2. Then we can define the map

$$\varphi_\alpha : \text{Aut}(F_1) \to \text{Aut}(F_2),\ \sigma = (\sigma_X)_{X\in \text{Ob}(\mathbf{C}_1)} \to (\alpha_X \circ \sigma_X \circ \alpha_X^{-1})_{X\in \text{Ob}(\mathbf{C}_1)}\ .$$

We claim that this map is an isomorphism of profinite groups. It is clearly bijective, with inverse

$$\varphi_\alpha^{-1} : \text{Aut}(F_2) \to \text{Aut}(F_1),\ \sigma = (\sigma_X)_{X\in \text{Ob}(\mathbf{C}_1)} \to (\alpha_X^{-1} \circ \sigma_X \circ \alpha_X)_{X\in \text{Ob}(\mathbf{C}_1)}\ .$$

If $\sigma = (\sigma_X)_{X\in \text{Ob}(\mathbf{C}_1)}, \tau = (\tau_X)_{X\in \text{Ob}(\mathbf{C}_1)} \in \text{Aut}(F_1)$, then

$$\begin{aligned} \varphi_\alpha(\sigma\tau) = \varphi_\alpha((\sigma_X \circ \tau_X)_{X\in \text{Ob}(\mathbf{C}_1)}) &= (\alpha_X \circ \sigma_X \circ \tau_X \circ \alpha^{-1})_{X\in \text{Ob}(\mathbf{C}_1)} = \\ &= ((\alpha_X \circ \sigma_X \circ \alpha^{-1}) \circ (\alpha\tau_X \circ \alpha^{-1}))_{X\in \text{Ob}(\mathbf{C}_1)} = \\ &= (\alpha_X \circ \sigma_X \circ \alpha^{-1})_{X\in \text{Ob}(\mathbf{C}_1)} (\alpha_X \circ \tau_X \circ \alpha^{-1})_{X\in \text{Ob}(\mathbf{C}_1)} = \varphi_\alpha(\sigma)\varphi_\alpha(\tau)\ . \end{aligned}$$

So φ_α is a group homomorphism. We prove now that it is continuous. For any object Y of $\mathbf{C}_1$, define $f_Y : \mathrm{Aut}(F_1) \to \mathrm{Aut}_{\mathbf{C}_2}(F_1(Y))$, $(\sigma_X)_{X\in\mathrm{Ob}(\mathbf{C}_1)} \mapsto \sigma_Y$ and $g_Y : \mathrm{Aut}(F_2) \to \mathrm{Aut}_{\mathbf{C}_2}(F_2(Y))$, $(\sigma_X)_{X\in\mathrm{Ob}(\mathbf{C}_1)} \mapsto \sigma_Y$. By definition of the topology on $\mathrm{Aut}(F_2)$, a subbase is given by

$$\left\{g_Y^{-1}(\{\tau\}) \mid Y \in \mathrm{Ob}(\mathbf{C}_1),\ \tau \in \mathrm{Aut}_{\mathbf{C}_2}(F_2(Y))\right\} .$$

For any object Y of $\mathbf{C}_1$ and for any $\tau \in \mathrm{Aut}_{\mathbf{C}_2}(F_2(Y))$, we have that

$$\begin{aligned}\varphi_\alpha^{-1}(g_Y^{-1}(\{\tau\})) &= (g_Y \circ \varphi_\alpha)^{-1}(\{\tau\}) = \\ &\{\sigma = (\sigma_X)_{X\in\mathrm{Ob}(\mathbf{C}_1)} \mid \alpha\circ\sigma_Y\circ\alpha^{-1} = (g_Y\circ\varphi_\alpha)(\sigma) = \tau\} = \\ &= \{\sigma = (\sigma_X)_{X\in\mathrm{Ob}(\mathbf{C}_1)} \mid \sigma_Y = \alpha^{-1}\circ\tau\circ\alpha\} = f_Y^{-1}(\{\alpha^{-1}\circ\tau\circ\alpha\}) ,\end{aligned}$$

which is open by definition of the topology on $\mathrm{Aut}(F_1)$. So φ_α is continuous. In the same way, one can show that φ_α^{-1} is continuous. So φ_α is an isomorphism of topological groups, as we wanted.
It is clear from the definition of φ_α that it depends on the isomorphism α. Let $\beta : F_1 \to F_2$ be another isomorphism, i.e. we have isomorphisms $\beta_X : F_1(X) \to F_2(X)$ (for any object X of $\mathbf{C}_1$) that are compatible with each other in the same sense as above. Then $\beta^{-1}\alpha = (\beta_X \circ \alpha_X^{-1})_{X\in\mathrm{Ob}(\mathbf{C}_1)}$ is an automorphism of the functor F_1 (for any X, $\beta_X^{-1}\circ\alpha_X : F_1(X) \to F_1(X)$ is an isomorphism and these isomorphisms are compatible). Define

$$\gamma_{\beta^{-1}\alpha} : \mathrm{Aut}(F_1) \to \mathrm{Aut}(F_1),\ \sigma \mapsto (\beta^{-1}\alpha)\sigma(\beta^{-1}\alpha)^{-1}$$

(conjugation by $\beta^{-1}\alpha$). Then $\gamma_{\beta^{-1}\alpha}$ is an inner automorphism of $\mathrm{Aut}(F_1)$. For any $\sigma = (\sigma_X)_{X\in\mathrm{Ob}(\mathbf{C}_1)}$ we have that

$$\begin{aligned}\varphi_\beta(\sigma) &= (\beta_X\circ\sigma_X\circ\beta_X^{-1})_{X\in\mathrm{Ob}(\mathbf{C}_1)} = \\ &= \left(\alpha_X\circ(\alpha_X^{-1}\circ\beta_X\circ\sigma_X\circ\beta_X^{-1}\circ\alpha_X\right)\circ\alpha_X^{-1})_{X\in\mathrm{Ob}(\mathbf{C}_1)} = \\ &\qquad \varphi_\alpha\left((\alpha_X^{-1}\circ\beta_X\circ\sigma_X\circ\beta_X^{-1}\circ\alpha_X)_{X\in\mathrm{Ob}(\mathbf{C}_1)}\right) = \varphi_\alpha(\gamma_{\beta^{-1}\alpha}(\sigma)) .\end{aligned}$$

Hence $\varphi_\beta = \varphi_\alpha \circ \gamma_{\beta^{-1}\alpha}$. □

Theorem 1.4.34 (Main theorem about Galois categories). *Let $\mathbf{C}$ be an essentially small Galois category with fundamental functor F. Then:*

*(a) if π' is a profinite group and $G : \mathbf{C} \to \pi'$-**sets** is an equivalence of categories such that* for$' \circ G = F$, *where* for$' : \pi'$-**sets** $\to$ **sets** *is the forgetful functor, then $\pi' \cong \mathrm{Aut}(F)$ as profinite groups;*

*(b) the functor $H' : \mathbf{C} \to \mathrm{Aut}(F)$-**sets** defined in lemma 1.4.29 is an equivalence of categories;*

*(c) if $F' : \mathbf{C} \to$ **sets** is another fundamental functor on $\mathbf{C}$, then F and F' are isomorphic;*

(d) *if* π' *is a profinite group such that* $\mathbf{C}$ *and* π'-**sets** *are equivalent, then* $\pi' \cong \mathrm{Aut}(F)$ *as profinite groups and the isomorphism is canonically determined up to an inner automorphism of* $\mathrm{Aut}(F)$.

Proof. (a) Applying the lemmas 1.4.24 and 1.4.32(3), we get that

$$\mathrm{Aut}(F) = \mathrm{Aut}(\mathrm{for}' \circ G) \cong \mathrm{Aut}(\mathrm{for}') \cong \pi' ,$$

as topological groups.

(b) By proposition 1.4.21, we have that the functor $H : \mathbf{C} \to \pi$-**sets** defined in lemma 1.4.2 is an equivalence of categories (here π is again the projective limit of the projective system of groups defined in proposition 1.3.14(3)). Moreover, by remark 1.4.3, we have that $\mathrm{for} \circ H = F$. By point (1), we have an isomorphism $\mathrm{Aut}(F) \cong \pi$, as profinite groups. This isomorphism induces a functor $H'' : \pi\text{-}\mathbf{sets} \to \mathrm{Aut}(F)\text{-}\mathbf{sets}$, which is clearly an isomorphism of categories (in particular an equivalence of categories) and by lemma 1.4.32 coincides with the functor defined applying lemma 1.4.29 to the Galois category π-**sets** (with fundamental functor the forgetful functor). We claim that $H' = H'' \circ H$. This is clear on morphisms, because $H'(f) = f = H''(f) = H''(H(f))$ for any morphism f. So we have to prove only that the effect on objects is the same, i.e. that the two actions of $\mathrm{Aut}(F)$ on $F(Y)$ coincide for any object Y. Let Y be an object of $\mathbf{C}$. Let $\sigma = (\sigma_X)_{X \in \mathrm{Ob}(\mathbf{C})} \in \mathrm{Aut}(F)$, $y \in F(Y)$. The functor H' gives us $\sigma y = \sigma_Y(y)$. On the other hand, by lemma 1.4.32(3), the functor $H'' \circ H$ gives us $\sigma.y = \varphi^{-1}(\sigma)y$, where $\varphi : \mathrm{Aut}(\mathrm{for}) \to \mathrm{Aut}(F)$ is the isomorphism defined as in lemma 1.4.24. Define $\tau = (\tau_X)_{X \in \mathrm{Ob}(\pi\text{-}\mathbf{sets})} := \varphi^{-1}(\sigma)$. This means that $(\sigma_X)_{X \in \mathrm{Ob}(\mathbf{C})} = \sigma = \varphi(\tau) = (\tau_{H(X)})_{X \in \mathrm{Ob}(\mathbf{C})}$. In particular, $\sigma_Y = \tau_{H(Y)}$. Then

$$\sigma y = \sigma_Y(y) = \tau_{H(Y)}(y) = \tau y = \varphi^{-1}(\sigma) y = \sigma.y .$$

This proves that $H'(Y) = H''(H(Y))$. So $H' = H'' \circ H'$ is an equivalence of categories, because it is the composition of two equivalences.

(c) Define J' in the same way as we defined J, but using the functor F' (see the lemmas 1.2.31 and 1.3.10 and the remarks 1.2.32(1) and 1.3.15(2)):

$$J' = \{[(A, a)]_{\sim'} \mid A \text{ Galois, } a \in F'(A)\} ,$$

where $[(A, a)] \sim' [(B, b)]$ if and only there exists an isomorphism $f : A \to B$ such that $F'(f)(a) = b$ and $[(A, a)]_{\sim'} \geq [(B, b)]_{\sim'}$ if and only if there exists a morphism $f : A \to B$ such that $F'(f)(a) = b$. By corollary 1.3.11, we have that $F \cong \varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(A_j, -)$ and $F' \cong \varinjlim_{j \in J'} \mathrm{Hom}_{\mathbf{C}}(B_j, -)$, where for any $j \in J'$ we chose a pair (B_j, b_j) with B_j connected, $b_j \in F'(B_j)$ and $j = [(B_j, b_j)]_{\sim'}$ (if $j_1, j_2 \in J'$ and $j_1 \geq j_2$, we denote by $g_{j_1 j_2} : B_{j_1} \to B_{j_2}$ the unique morphism such that $g_{j_1 j_2}(b_{j_1}) = b_{j_2}$). So it is enough to prove that $\varinjlim_{j \in J} \mathrm{Hom}_{\mathbf{C}}(A_j, -) \cong \varinjlim_{j \in J'} \mathrm{Hom}_{\mathbf{C}}(B_j, -)$.
First of all, we will find an order isomorphism between J and J'. Let $j \in J$. Then $j = [(A_j, a_j)]_{\sim}$ and A_j is Galois, by remark 1.3.12. In particular, A_j is

not initial (remark 1.2.13(1)) and so $F'(A_j) \neq \emptyset$, by lemma 1.2.17 applied to the fundamental functor F'. Choose $a'_j \in F'(A_j)$. Then $[(A_j, a'_j)]_{\sim'} \in J'$ (recall that the fact of being Galois does not depend on the fundamental functor, by remark 1.3.2(2)). So we can define the map

$$\alpha : J \to J',\ j \mapsto [(A_j, a'_j)]_{\sim'} .$$

We claim that α is bijective. Let $j_1, j_2 \in J$ be such that $\alpha(j_1) = \alpha(j_2)$, i.e. $[(A'_{j_1}, a'_{j_1})]_{\sim'} = [(A_{j_2}, a'_{j_2})]_{\sim'}$. This means that there exists an isomorphism $f : A_{j_1} \to A_{j_2}$ such that $F'(f)(a'_{j_1}) = a'_{j_2}$. Consider $F(f)(a_{j_1}) \in F(A_{j_2})$. Since A_{j_2} is Galois, by lemma 1.3.4 the action of $\mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ on $F(A_{j_2})$ is transitive. So there exists $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ such that $a_{j_2} = F(\sigma)(F(f)(a_{j_1})) = F(\sigma \circ f)(a_{j_1})$. This shows that $j_1 = [(A_{j_1}, a_{j_1})]_\sim = [(A_{j_2}, j_2)]_\sim = j_2$. So α is injective.
Let $k \in J'$. Since $k = [(B_k, b_k)]_{\sim'} \in J'$, we have that B_k is Galois, by remark 1.3.12. Moreover, $F(B_k) \neq \emptyset$ (because B_k connected implies B_k not initial, see remark 1.2.13(1) and lemma 1.2.17). Choose $b \in F(B_k)$ and define $j := [(B_k, b)]_\sim \in J$. From $[(A_j, a_j)]_\sim = j = [(B_k, b)]_\sim$ it follows that there exists an isomorphism $f : A_j \to B_k$ such that $F(f)(a_j) = b_j$. Consider $F'(f)(a'_j) \in F'(B_k)$. Since B_k is Galois, the action of $\mathrm{Aut}_{\mathbf{C}}(B_k)$ on $F'(B_k)$ is transitive, by lemma 1.3.4 apllied to the fundamental functor F'. So there exists $\sigma \in \mathrm{Aut}_{\mathbf{C}}(B_k)$ such that $b = F'(\sigma)(F'(f)(a'_j)) = F'(\sigma \circ f)(a'_j)$. This shows that $[(B_k, b)]_{\sim'} = [(A_j, a'_j)]_{\sim'} = \alpha(j)$. Then α is surjective.
We prove now that, for any $j_1, j_2 \in J$, $\alpha(j_1) \geq \alpha(j_2)$ if and only if $j_1 \geq j_2$. Assume that $j_1 \geq j_2$, i.e. $[(A_{j_1}, a_{j_1})]_\sim \geq [(A_{j_2}, a_{j_2})]_\sim$. This means that there exists a morphism $f : A_{j_1} \to A_{j_2}$ such that $F(f)(a_{j_1}) = F(f)(a_{j_2})$. Consider $F'(f)(a'_{j_1}) \in F'(A_{j_2})$. Since A_{j_2} is Galois, by lemma 1.3.4 the action of $\mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ on $F'(A_{j_2})$ is transitive. So there exists $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ such that $a'_{j_2} = F'(\sigma)(F'(f)(a'_{j_1})) = F'(\sigma \circ f)(a'_{j_1})$. This shows that $\alpha(j_1) = [(A_{j_1}, a'_{j_1})]_{\sim'} \geq [(A_{j_2}, a'_{j_2})]_{\sim'} = \alpha(j_2)$.
Conversely, assume $\alpha(j_1) \geq \alpha(j_2)$, i.e. $[(A'_{j_1}, a'_{j_1})]_{\sim'} \geq [(A_{j_2}, a'_{j_2})]_{\sim'}$. This means that there exists an morphism $f : A_{j_1} \to A_{j_2}$ such that $F'(f)(a'_{j_1}) = a'_{j_2}$. Consider $F(f)(a_{j_1}) \in F(A_{j_2})$. Since A_{j_2} is Galois, by lemma 1.3.4 the action of $\mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ on $F(A_{j_2})$ is transitive. So there exists $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A_{j_2})$ such that $a_{j_2} = F(\sigma)(F(f)(a_{j_1})) = F(\sigma \circ f)(a_{j_1})$. This shows that $j_1 = [(A_{j_1}, a_{j_1})]_\sim \geq [(A_{j_2}, a_{j_2})]_\sim = j_2$.
Notice that for any $j \in J$ we have

$$[(A_j, a'_j)]_{\sim'} = \alpha(j) = [(B_{\alpha(j)}, b_{\alpha(j)})]_{\sim'} .$$

In particular, $A_j \cong B_{\alpha(j)}$. We want to find isomorphisms $h_j : A_j \to B_{\alpha(j)}$ (for any $j \in J$) in a way that is compatible with the morphisms $f_{j_1 j_2}$ and $g_{\alpha(j_1)\alpha(j_2)}$, i.e. we would like to have $g_{\alpha(j_1)\alpha(j_2)} \circ h_{j_1} = h_{j_2} \circ f_{j_1 j_2}$ for any $j_1, j_2 \in J$ with $j_1 \geq j_2$. For any $j \in J$, let S_j be the set of isomorphisms from A_j to $B_{\alpha(j)}$, which is non-empty because $A_j \cong B_{\alpha(j)}$. Notice that $\mathrm{Hom}_{\mathbf{C}}(A_j, B_{\alpha(j)})$ is finite, because we have that $\psi^{B_{\alpha(j)}}_{(A_j, a_j)} : \mathrm{Hom}_{\mathbf{C}}(A_j, B_{\alpha(j)}) \to F(B_{\alpha(j)})$ is injective (lemma 1.2.30) and $F(B_{\alpha(j)})$ is a finite set. So $S_j \subseteq \mathrm{Hom}_{\mathbf{C}}(A_j, B_{\alpha(j)})$ is also finite, for any $j \in J$. Consider the discrete topology on each S_j and the product topology on $\prod_{j \in J} S_j$. Then S_j is compact for any $j \in J$, because it is finite, and so the product is compact by Tichonov's theorem. For any $j_1, j_2 \in J$ with $j_1 \geq j_2$, define

$$T_{j_1 j_2} := \left\{ (h_j)_{j \in J} \in \prod_{j \in J} S_j \;\middle|\; g_{\alpha(j_1)\alpha(j_2)} \circ h_{j_1} = h_{j_2} \circ f_{j_1 j_2} \right\} \subseteq \prod_{j \in J} S_j \;.$$

We claim that $T := \bigcap_{j_1, j_2 \in J, j_1 \geq j_2} T_{j_1 j_2} \neq \emptyset$. For any $k \in J$, define $p_k : \prod_{j \in J} S_j \to S_k$ to be the canonical projection, which is continuous by definition of product topology. Let $j_1, j_2 \in J$ be such that $j_1 \geq j_2$. If we consider the discrete topology on $\mathrm{Hom}_{\mathbf{C}}(A_j, B_{\alpha(j)})$ for any j, then also the maps

$$f^*_{j_1 j_2} : \mathrm{Hom}_{\mathbf{C}}(A_{j_2}, B_{\alpha(j_2)}) \to \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)}),\ h \mapsto h \circ f_{j_1 j_2}$$

and

$$g_{\alpha(j_1)\alpha(j_2)*} : \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_1)}) \to \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)}),\ h \mapsto g_{\alpha(j_1)\alpha(j_2)} \circ h$$

are continuous. Then, considering the product topology (which is again the discrete topology) on $\mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)}) \times \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)})$, the map

$$\begin{aligned} q_{j_1 j_2} : \prod_{j \in J} S_j &\to \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)}) \times \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)}), \\ (h_j)_{j \in J} &\mapsto \left(g_{\alpha(j_1)\alpha(j_2)} \circ h_{j_1}, h_{j_2} \circ f_{j_1 j_2} \right) \end{aligned}$$

is continuous, because its components are $g_{\alpha(j_1)\alpha(j_2)*} \circ p_{j_1}$ and $f^*_{j_1 j_2} \circ p_{j_2}$, which are compositions of continuous functions. Define

$$\begin{aligned} \Delta_{j_1 j_2} := \{(h, h) \mid h \in \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)})\} \subseteq& \\ \subseteq \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)}) \times \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)}) \;.& \end{aligned}$$

Then $\Delta_{j_1 j_2}$ is closed, because $\mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)}) \times \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, B_{\alpha(j_2)})$ has the discrete topology. We have that $T_{j_1 j_2} = q^{-1}_{j_1 j_2}(\Delta_{j_1 j_2})$. So $T_{j_1 j_2}$ is closed and this holds for any $j_1, j_2 \in J$ with $j_1 \geq j_2$. Then, by the compactness of $\prod_{j \in J} S_j$, in order to show that $T \neq \emptyset$ it is enough to prove that $T_{j_1 k_1} \cap \cdots \cap T_{j_n k_n} \neq \emptyset$ for any $n \in \mathbb{N}$, $j_1, \ldots, j_n, k_1, \ldots, k_n \in J$ with $j_i \geq k_i$ for every $i = 1, \ldots, n$. Fix such $j_1, \ldots, j_n, k_1, \ldots, k_n \in J$. Since J is directed (lemma 1.3.10), there exists $k \in J$ such that $k \geq j_i$ for any $i = 1, \ldots, n$. Then, by transitivity, we have also that $k \geq k_i$ for any $i = 1, \ldots, n$. Notice that these inequalities are preserved by α. We know that S_k is non-empty, so we can fix an $h_k \in S_k$. For any $k' \in J$ with $k \geq k'$, we have the following diagram.

$$\begin{array}{ccc} A_k & \xrightarrow{f_{kk'}} & A_{k'} \\ {\scriptstyle h_k}\downarrow & & \vdots\, ? \\ B_{\alpha(k)} & \xrightarrow{g_{\alpha(k)\alpha(k')}} & B_{\alpha(k')} \end{array}$$

Fix any $h \in S_{k'}$ (recall that we know that $S_{k'} \neq \emptyset$) and consider $F(h \circ f_{kk'})(a_k), F(g_{\alpha(k)\alpha(k')} \circ h_k)(a_k) \in F(B_{\alpha(k')})$. Since $[(B_{\alpha(k')}, b_{\alpha(k')})]_{\sim'} = \alpha(k') \in J'$, we have that $B_{\alpha(k')}$ is Galois, by remark 1.3.12. Then $\mathrm{Aut}_{\mathbf{C}}(B_{\alpha(k')})$ acts freely and transitively on $F(B_{\alpha(k')})$, by lemma 1.3.4. So there exists a unique $\sigma \in \mathrm{Aut}_{\mathbf{C}}(B_{\alpha(k')})$ such that $F(g_{\alpha(k)\alpha(k')} \circ h_k)(a_k) = F(\sigma)(F(h \circ f_{kk'})(a_k)) = F(\sigma \circ h \circ f_{kk'})(a_k)$. This means that $\psi^{B_{\alpha(k')}}_{(A_k,a_k)}(g_{\alpha(k)\alpha(k')} \circ h_k) = \psi^{B_{\alpha(k')}}_{(A_k,a_k)}(\sigma \circ h \circ f_{kk'})$. But $\psi^{B_{\alpha(k')}}_{(A_k,a_k)}$ is injective by lemma 1.2.30, because A_k is connected. So we must have $g_{\alpha(k)\alpha(k')} \circ h_k = \sigma \circ h \circ f_{kk'}$. We can define $h_{k'} := \sigma \circ h : A_{k'} \to B_{\alpha(k')}$. Then $h_{k'}$ is an isomorphism, because it is a composition of isomorphisms. So $h_{k'} \in S_{k'}$. Moreover, $g_{\alpha(k)\alpha(k')} \circ h_k = h_{k'} \circ f_{kk'}$. We have that $h_{k'}$ is the unique isomorphism with this property. Indeed, if $\widetilde{h_{k'}} \in S_{k'}$ satisfies $g_{\alpha(k)\alpha(k')} \circ h_k = \widetilde{h_{k'}} \circ f_{kk'}$, we can define $\widetilde{\sigma} = \widetilde{h_{k'}} \circ h^{-1} : B_{\alpha(k')} \to B_{\alpha(k')}$, which is an isomorphism because it is a composition of isomorphisms. So $\widetilde{\sigma} \in \mathrm{Aut}_{\mathbf{C}}(B_{\alpha(k')})$. Moreover, $\widetilde{h_{k'}} = \widetilde{\sigma} \circ h$. Then

$$F(\widetilde{\sigma})(F(h \circ f_{kk'})(a_k)) = F(\widetilde{\sigma} \circ h \circ f_{kk'})(a_k) = \\ = F(\widetilde{h_{k'}} \circ f_{kk'})(a_k) = F(g_{\alpha(k)\alpha(k')} \circ h_k)(a_k) \ .$$

This implies that $\widetilde{\sigma} = \sigma$ and so $\widetilde{h_{k'}} = \sigma \circ h = h_{k'}$. Notice that if $k' = k$ we get the same morphism we started with. For any $k' > k$, choose $h_{k'} \in S_{k'}$ arbitrarily (we can do it because $S_{k'} \neq \emptyset$). So we have defined an element $(h_j)_{j \in J}$ of the product $\prod_{j \in J} S_j$. We claim that $(h_j)_{j\in J} \in T_{j_1k_1} \cap \cdots \cap T_{j_nk_n}$. Let $i \in \{1, \ldots, n\}$. By lemma 1.2.33, we have that $f_{kk_i} = f_{j_ik_i} \circ f_{jj_i}$ and $g_{\alpha(k)\alpha(k_i)} = g_{\alpha(j_i)\alpha(k_i)} \circ g_{\alpha(j)\alpha(j_i)}$. So

$$h_{k_i} \circ f_{j_ik_i} \circ f_{kj_i} = h_{k_i} \circ f_{kk_i} = g_{\alpha(k)\alpha(k_i)} \circ h_k = \\ = g_{\alpha(j_i)\alpha(k_i)} \circ g_{\alpha(k)\alpha(j_i)} \circ h_k = g_{\alpha(j_i)\alpha(k_i)} \circ h_{j_i} \circ f_{kj_i} \ .$$

By lemma 1.3.9, $f_{kj_i} : A_k \to A_{j_i}$ is an epimorphism, because A_{j_i} is connected and A_k is not initial. So we must have $h_{k_i} \circ f_{j_ik_i} = g_{\alpha(j_i)\alpha(k_i)} \circ h_{j_i}$. This means that $(h_j)_{j\in J} \in T_{j_ik_i}$. Then $(h_j)_{j\in J} \in T_{j_1k_1} \cap \cdots \cap T_{j_nk_n}$. In particular, $T_{j_1k_1} \cap \cdots \cap T_{j_nk_n} \neq \emptyset$, which is what we needed. So $T \neq \emptyset$. Fix $(h_j)_{j\in J} \in T$. Let now X be an object of $\mathbf{C}$. For any $j \in J$, the isomorphism h_j gives rise to a bijection

$$h_j^* : \mathrm{Hom}_{\mathbf{C}}(B_{\alpha(j)}, X) \to \mathrm{Hom}_{\mathbf{C}}(A_j, X), \ f \mapsto f \circ h_j \ .$$

If $j_1, j_2 \in J$ are such that $j_1 \geq j_2$, then the following diagram is commutative, because $h_{j_2} \circ f_{j_1j_2} = g_{\alpha(j_1)\alpha(j_2)} \circ h_{j_1}$.

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{C}}(B_{\alpha(j_1)}, X) & \xrightarrow{h_{j_1}^*} & \mathrm{Hom}_{\mathbf{C}}(A_{j_1}, X) \\ \uparrow g^*_{\alpha(j_1)\alpha(j_2)} & & \uparrow f^*_{j_1j_2} \\ \mathrm{Hom}_{\mathbf{C}}(B_{\alpha(j_2)}, X) & \xrightarrow{h_{j_2}^*} & \mathrm{Hom}_{\mathbf{C}}(A_{j_2}, X) \end{array}$$

Then we can use the universal property of the injective limit to get a bijection

$\Phi_X : \varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(B_{\alpha(j)}, X) \to \varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, X)$. Since $\alpha : J \to J'$ is an order isomorphism, we have that

$$\varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(B_{\alpha(j)}, X) = \varprojlim_{j\in J'} \mathrm{Hom}_{\mathbf{C}}(B_j, X) .$$

So we have a bijection $\Phi_X : \varprojlim_{j\in J'} \mathrm{Hom}_{\mathbf{C}}(B_j, X) \to \varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, X)$. It remains to prove that these bijections are compatible with morphisms, i.e. that for any morphism $h : X \to Y$ we have

$$\Phi_Y \circ \varprojlim_{j\in J'} \mathrm{Hom}_{\mathbf{C}}(B_j, h) = \varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h) \circ \Phi_X .$$

Let $X \in \varprojlim_{j\in J'} \mathrm{Hom}_{\mathbf{C}}(B_j, X)$. Then there exist $k \in J'$ and $f \in \mathrm{Hom}_{\mathbf{C}}(B_k, X)$ such that $X = [f]_\sim$. We have that

$$\left(\Phi_Y \circ \varprojlim_{j\in J'} \mathrm{Hom}_{\mathbf{C}}(B_j, h)\right)[X] = \left(\Phi_Y \circ \varprojlim_{j\in J'} \mathrm{Hom}_{\mathbf{C}}(B_j, h)\right)([f]_\sim) =$$
$$= \Phi_Y\left([h\circ f]_\sim\right) = [h^*_{\alpha^{-1}(k)}(h\circ f)]_\sim = [h \circ f \circ h_{\alpha^{-1}(k)}]_\sim =$$
$$= \varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h)\left([f\circ h_{\alpha^{-1}(k)}]_\sim\right) = \varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h)\left([h^*_{\alpha^{-1}(k)}(f)]_\sim\right) =$$
$$= \left(\varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h) \circ \Phi_X\right)([f]_\sim) = \left(\varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, h) \circ \Phi_X\right)(X) .$$

This proves the compatibility condition. So

$$\varprojlim_{j\in J} \mathrm{Hom}_{\mathbf{C}}(A_j, -) \cong \varprojlim_{j\in J'} \mathrm{Hom}_{\mathbf{C}}(B_j, -) ,$$

which is what we wanted.

(d) Let $G : \mathbf{C} \to \pi'$**-sets** be an equivalence of categories and let $\mathrm{for}' : \pi'$**-sets** $\to$ **sets** be the forgetful functor. Consider the functor $F' := \mathrm{for}' \circ G : \mathbf{C} \to$ **sets**. We claim that F' is a fundamental functor on $\mathbf{C}$. Recall that π'**-sets** is a Galois category with fundamental functor for'. Then for' satisfies (G4), (G5) and (G6) of the definition.
Let X, Y, S be objects of $\mathbf{C}_1$, with two morphisms $f_1 : X \to S$, $f_2 : Y \to S$. Consider the fibred product $G(X) \times_{G(S)} G(Y)$ in π'**-sets**, together with the projections $p_1 : G(X)\times_{G(S)} G(Y) \to G(X)$ and $p_1 : G(X)\times_{G(S)} G(Y) \to G(Y)$. By definition of fibred product, $G(f_1)\circ p_1 = G(f_2)\circ p_2$. Since G is an equivalence of categories, it is essentially surjective (lemma 1.4.5). Then there exists an object Z of $\mathbf{C}_1$ with $G(Z) \cong G(X) \times_{G(S)} G(Y)$. Let $\varphi : G(Z) \to G(X) \times_{G(S)} G(Y)$ be an isomorphism. Consider the morphisms $p_1 \circ \varphi : G(Z) \to G(X)$, $p_2 \circ \varphi : G(Z) \to G(Y)$. Since G is an equivalence, it is full (lemma 1.4.5). So there exist morphisms $q_1 : Z \to X$, $q_2 : Z \to Y$ such that $G(q_1) = p_1 \circ \varphi$ and $G(q_2) = p_2 \circ \varphi$. We have that

$$G(f_1 \circ q_1) = G(f_1) \circ G(q_1) = G(f_1) \circ p_1 \circ \varphi =$$
$$= G(f_2) \circ p_2 \circ \varphi = G(f_2) \circ G(q_2) = G(f_2 \circ q_2) .$$

Since G is an equivalence of categories, it is faithful (lemma 1.4.5). So we must have $f_1 \circ q_1 = f_2 \circ q_2$. Moreover, let W be an object of $\mathbf{C}$ with two morphisms $g_1 : W \to X$, $g_2 : W \to Y$ such that $f_1 \circ g_1 = f_2 \circ g_2$. Then $G(f_1) \circ G(g_1) = G(f_1 \circ g_1) = G(f_2 \circ g_2) = G(f_2) \circ G(g_2)$. By the universal property of the fibred product, there exists a unique morphism $h : G(W) \to G(X) \times_{G(S)} G(Y)$ with $p_1 \circ h = G(g_1)$ and $p_2 \circ h = G(g_2)$. Consider the morphism $\varphi^{-1} \circ h : G(W) \to G(Z)$. Since G is fully faithful, there exists a unique morphism $g : W \to Z$ such that $G(g) = \varphi^{-1} \circ h$. Then we have

$$G(q_1 \circ g) = G(q_1) \circ G(g) = p_1 \circ \varphi \circ \varphi^{-1} \circ h = p_1 \circ h = G(g_1)$$

and

$$G(q_2 \circ g) = G(q_2) \circ G(g) = p_2 \circ \varphi \circ \varphi^{-1} \circ h = p_2 \circ h = G(g_2) \ .$$

Since G is faithful, this implies $q_1 \circ g = g_1$ and $q_2 \circ g = g_2$. If $\widetilde{g} : W \to Z$ satisfies $q_1 \circ \widetilde{g} = g_1$ and $q_2 \circ \widetilde{g} = g_2$, then $G(g_1) = G(q_1 \circ \widetilde{g}) = G(q_1) \circ G(\widetilde{g}) = p_1 \circ \varphi \circ G(\widetilde{g})$ and $G(g_2) = G(q_2 \circ \widetilde{g}) = G(q_2) \circ G(\widetilde{g}) = p_2 \circ \varphi \circ G(\widetilde{g})$. By uniqueness of h, we must have $\varphi \circ G(\widetilde{g}) = h$. So $G(\widetilde{g}) = \varphi^{-1} \circ h$. By uniqueness of g, we must have $\widetilde{g} = g$. This proves that Z is a fibred product of X and Y over S. So $X \times_S Y \cong Z$ and $G(X \times_S Y) \cong G(Z) \cong G(Z) \times_{G(S)} G(Y)$. Then G preserves fibred products. By (G4) of the definition of Galois category, we have that for$'$ preserves fibred products too. So $F' = \text{for}' \circ G$ preserves fibred products. In the same way, it can be proved that F' preserves terminal objects, finite sums and quotients by finite groups of automorphisms. So F' satisfies (G4).
Let $f : X \to Y$ be an epimorphism in $\mathbf{C}$. Let Z be an object of π'**-sets** and let $g_1, g_2 : G(Y) \to Z$ be two morphisms such that $g_1 \circ G(f) = g_2 \circ G(f)$. Since G is essentially surjective, there exists an object W of $\mathbf{C}$ such that $Z \cong G(W)$. Let $\varphi : Z \to G(W)$ be an isomorphism. Consider the morphisms $\varphi \circ g_1 : G(Y) \to G(W)$ and $\varphi \circ g_2 : G(Y) \to G(W)$. Since G is full, there exist two morphisms $h_1, h_2 : Y \to W$ with $G(h_1) = \varphi \circ g_1$ and $G(h_2) = \varphi \circ g_2$. We have that

$$\begin{aligned} G(h_1 \circ f) = G(h_1) \circ G(f) = \varphi \circ g_1 \circ G(f) = \\ = \varphi \circ g_2 \circ G(f) = G(h_2) \circ G(f) = G(h_2 \circ f) \ . \end{aligned}$$

Since G is faithful, this implies that $h_1 \circ f = h_2 \circ f$. But f is an epimorphism, so we must have $h_1 = h_2$. Then $g_1 = \varphi^{-1} \circ G(h_1) = \varphi^{-1} \circ G(h_2) = g_2$. This proves that $G(f)$ is an epimorphism. Then, by (G5) of the definition of Galois category, we have that $F'(f) = \text{for}'(G(f))$ is an epimorphism. So F' satisfies (G5).
Finally, let $f : X \to Y$ be a morphism in $\mathbf{C}$ such that $F'(f) = \text{for}'(G(f))$ is an isomorphism. By (G6) of the definition of Galois category, we have that $G(f) : G(X) \to G(Y)$ is an isomorphism in π**-sets**. So we can consider the morphism $G(f)^{-1} : G(Y) \to G(X)$. Since G is full, there exists a morphism $g : Y \to X$ such that $G(g) = G(f)^{-1}$. We have that $G(f \circ g) = G(f) \circ G(g) = G(f) \circ G(f)^{-1} = \text{id}_{G(Y)} = G(\text{id}_Y)$ and $G(g \circ f) = G(g) \circ G(f) = G(f)^{-1} \circ G(f) = \text{id}_{G(X)} = G(\text{id}_X)$. Since G is faithful, this

implies $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. So f is an isomorphism. This proves that F' satisfies (G6).
So F' is a fundamental functor. By point (c), we have that F and F' are isomorphic. Then, by lemma 1.4.33, we have an isomorphism of profinite groups between $\mathrm{Aut}(F)$ and $\mathrm{Aut}(F')$ and this isomorphism is canonically determined up to an inner automorphism of $\mathrm{Aut}(F)$. On the other hand, applying the lemmas 1.4.24 and 1.4.32(3), we have that $\mathrm{Aut}(F') = \mathrm{Aut}(G \circ \mathrm{for}') \cong \mathrm{Aut}(\mathrm{for}') \cong \pi'$ as profinite groups (and all the isomorphisms involved are canonical). This ends the proof.

□

Definition 1.4.35. Given a Galois category $\mathbf{C}$ with fundamental functor F, we define $\pi(\mathbf{C}, F) := \mathrm{Aut}(F)$ and we call this profinite group the *fundamental group* of $\mathbf{C}$ with respect to F.

From the main theorem about Galois categories, it follows that the fundamental group of a Galois category, up to isomorphism, does not depend on the fundamental functor. We conclude with a lemma which can be used to show that the construction of the fundamental group of a connected scheme is functorial (see remark 2.3.14).

Lemma 1.4.36. *Let $\mathbf{D}$ be a category such that we can associate to any object X of $\mathbf{D}$ an essentially small Galois category $\mathbf{C}_X$ with fundamental functor $F_X : \mathbf{C}_X \to$ **sets** and to any morphism $f : X \to Y$ in $\mathbf{D}$ a functor $G_f : \mathbf{C}_Y \to \mathbf{C}_X$ with an isomorphism of functors $\alpha_f = (\alpha_{f,B})_{B \in \mathrm{Ob}(\mathbf{C}_Y)} : F_X \circ G_f \to F_Y$. Assume that:*

(1) for any object X of $\mathbf{D}$ we have an isomorphism of functors

$$\beta_X = (\beta_{X,A})_{A \in \mathrm{Ob}(\mathbf{C}_X)} : G_{\mathrm{id}_X} \to \mathrm{id}_{\mathbf{C}_X}$$

such that $F_X(\beta_{X,A}) = \alpha_{\mathrm{id}_X, A}$ for any object A of $\mathbf{C}_X$;

(2) for any two morphisms $f : X \to Y$, $g : Y \to Z$ in $\mathbf{D}$ we have an isomorphism of functors $\gamma_{f,g} = (\gamma_{f,g,C})_{C \in \mathrm{Ob}(\mathbf{C}_Z)} : G_f \circ G_g \to G_{g \circ f}$ such that the following diagram in **sets** *is commutative for any object C of $\mathbf{C}_Z$.*

$$\begin{array}{ccc} (F_X \circ G_f \circ G_g)(C) & \xrightarrow{\alpha_{f,G_g(C)}} & (F_Y \circ G_g)(C) \\ {\scriptstyle F_X(\gamma_{f,g,C})}\downarrow & & \downarrow{\scriptstyle \alpha_{g,C}} \\ (F_X \circ G_{g\circ f})(C) & \xrightarrow{\alpha_{g\circ f,C}} & F_Z(C) \end{array}$$

*If for any object X of $\mathbf{C}$ we define $\pi(X) := \pi(\mathbf{C}_X, F_X) = \mathrm{Aut}(F_X)$, then we can extend π to a functor $\mathbf{D} \to$ **Prof**, where **Prof** is the category of profinite groups, with morphisms given by continuous group homomorphisms.*

Proof. Let $f : X \to Y$ be a morphism in $\mathbf{D}$. Define

$$\begin{aligned} \pi(f) : \pi(X) = \mathrm{Aut}(F_X) &\to \pi(Y) = \mathrm{Aut}(F_Y), \\ \sigma = (\sigma_A)_{A \in \mathrm{Ob}(\mathbf{C}_X)} &\mapsto (\alpha_{f,B} \circ \sigma_{G_f(B)} \circ \alpha_{f,B}^{-1})_{B \in \mathrm{Ob}(\mathbf{C}_Y)} \,. \end{aligned}$$

First of all, we check that $\pi(f)$ is well defined, i.e. that $\pi(f)(\sigma)$ is indeed an automorphism of F_Y, for any automorphism σ of F_X. Let $\sigma = (\sigma_A)_{A\in \mathrm{Ob}(\mathbf{C}_X)} \in \mathrm{Aut}(F_X)$. For any object B of $\mathbf{C}_Y$, we have that $\alpha_{f,B} \circ \sigma_{G_f(B)} \circ \alpha_{f,B}^{-1} : F_Y(B) \to F_Y(B)$ is a bijection, because it is a composition of bijections. We have to check that the compatibility condition is satisfied. Let $h : B_1 \to B_2$ be a morphism in $\mathbf{C}_Y$. Since α_f is an isomorphism of functors, then also $\alpha_f^{-1} = (\alpha_{f,B}^{-1})_{B\in \mathbf{C}_Y}$ is an isomorphism of functors. Applying this and the fact that σ is an automorphism of F_X, we get that

$$\begin{aligned}&\alpha_{f,B_2} \circ \sigma_{G_f(B_2)} \circ \alpha_{f,B_2}^{-1} \circ F_Y(h) = \alpha_{f,B_2} \circ \sigma_{G_f(B_2)} \circ F_Y(h) \circ \alpha_{f,B_1}^{-1} = \\ &\quad = \alpha_{f,B_2} \circ F_Y(h) \circ \sigma_{G_f(B_1)} \circ \alpha_{f,B_1}^{-1} = F_Y(h) \circ \alpha_{f,B_1} \circ \sigma_{G_f(B_1)} \circ \alpha_{f,B_1}^{-1} .\end{aligned}$$

This shows that $\pi(f)(\sigma) = (\alpha_{f,B} \circ \sigma_{G_f(B)} \circ \alpha_{f,B}^{-1})_{B\in \mathrm{Ob}(\mathbf{C}_Y)}$ is an automorphism of F_Y. We prove now that $\pi(f)$ is a group homomorphism. Let $\sigma = (\sigma_A)_{A\in \mathrm{Ob}(\mathbf{C}_X)}, \tau = (\tau_A)_{A\in \mathrm{Ob}(\mathbf{C}_X)} \in \mathrm{Aut}(F_X)$. Then

$$\begin{aligned}&\pi(f)(\sigma\tau) = \pi(f)\left((\sigma_A \circ \tau_A)_{A\in \mathrm{Ob}(\mathbf{C}_X)}\right) = (\alpha_{f,B} \circ \sigma_{G_f(B)} \circ \tau_{G_f(B)} \circ \alpha_{f,B}^{-1})_{B\in \mathrm{Ob}(\mathbf{C}_Y)} = \\ &\quad = (\alpha_{f,B} \circ \sigma_{G_f(B)} \circ \alpha_{f,B}^{-1} \circ \alpha_{f,B} \circ \tau_{G_f(B)} \circ \alpha_{f,B}^{-1})_{B\in \mathrm{Ob}(\mathbf{C}_Y)} = \\ &= (\alpha_{f,B} \circ \sigma_{G_f(B)} \circ \alpha_{f,B}^{-1})_{B\in \mathrm{Ob}(\mathbf{C}_Y)} (\alpha_{f,B} \circ \tau_{G_f(B)} \circ \alpha_{f,B}^{-1})_{B\in \mathrm{Ob}(\mathbf{C}_Y)} = \pi(f)(\sigma)\pi(f)(\tau) .\end{aligned}$$

So $\pi(f)$ is a group homomorphism. We check now that $\pi(f)$ is continuous. For any object A_0 of $\mathbf{C}_X$, define

$$p_{A_0} : \mathrm{Aut}(F_X) \to \mathrm{S}_{F_X(A_0)},\ \sigma = (\sigma_A)_{A\in \mathrm{Ob}(\mathbf{C}_X)} \mapsto \sigma_{A_0} .$$

Analogously, for any object B_0 of $\mathbf{C}_Y$, define

$$q_{B_0} : \mathrm{Aut}(F_Y) \to \mathrm{S}_{F_Y(B_0)},\ \sigma = (\sigma_B)_{B\in \mathrm{Ob}(\mathbf{C}_Y)} \mapsto \sigma_{B_0} .$$

By definition of the topology on $\mathrm{Aut}(F_Y)$ (see remark 1.4.23(3)), a base is given by

$$\{q_{B_0}^{-1}(\{\tau_0\}) \mid B_0 \in \mathrm{Ob}(\mathbf{C}_Y),\ \tau_0 \in \mathrm{S}_{F_Y(B_0)}\} .$$

Let B_0 be an object of $\mathbf{C}_Y$. For any $\sigma = (\sigma_A)_{A\in \mathrm{Ob}(\mathbf{C}_X)} \in \mathrm{Aut}(F_X)$, we have that

$$\begin{aligned}&(q_{B_0} \circ \pi(f))(\sigma) = q_{B_0}\left((\alpha_{f,B} \circ \sigma_{G_f(B)} \circ \alpha_{f,B}^{-1})_{B\in \mathrm{Ob}(\mathbf{C}_Y)}\right) = \\ &\qquad = \alpha_{f,B_0} \circ \sigma_{G_f(B_0)} \circ \alpha_{f,B_0}^{-1} = \alpha_{f,B_0} \circ p_{G_f(B_0)}(\sigma) \circ \alpha_{f,B_0}^{-1} .\end{aligned}$$

Then, for any $\tau_0 \in \mathrm{S}_{F_Y(B_0)}$,

$$\begin{aligned}&\pi(f)^{-1}(q_{B_0}^{-1}(\{\tau_0\})) = (q_{B_0} \circ \pi(f))^{-1}(\{\tau_0\}) = \\ &\quad = \{\sigma = (\sigma_A)_{A\in \mathrm{Ob}(\mathbf{C}_X)} \in \mathrm{Aut}(F_X) \mid \alpha_{f,B_0} \circ p_{G_f(B_0)}(\sigma) \circ \alpha_{f,B_0}^{-1} = \tau_0\} = \\ &\quad = \{\sigma = (\sigma_A)_{A\in \mathrm{Ob}(\mathbf{C}_X)} \in \mathrm{Aut}(F_X) \mid p_{G_f(B_0)}(\sigma) = \alpha_{f,B_0}^{-1} \circ \tau_0 \circ \alpha_{f,B_0}\} = \\ &\qquad = p_{G_f(B_0)}^{-1}(\{\alpha_{f,B_0}^{-1} \circ \tau_0 \circ \alpha_{f,B_0}\}) ,\end{aligned}$$

which by definition of the topology on $\mathrm{Aut}(F_X)$ (see remark 1.4.23(3)) implies that $\pi(f)^{-1}(q_{B_0}^{-1}(\{\tau_0\}))$ is open. Then $\pi(f)$ is continuous. So $\pi(f) : \pi(X) \to \pi(Y)$ is a morphism in **Prof**.
We check now that π is a functor. Let $X \in \mathrm{Ob}(\mathbf{D})$ and let $\sigma = (\sigma_A)_{A \in \mathrm{Ob}(\mathbf{C}_X)} \in \mathrm{Aut}(F_X)$. For any object A of $\mathbf{C}_X$, we have that

$$\alpha_{\mathrm{id}_X,A} \circ \sigma_{G_{\mathrm{id}_X}(A)} \circ \alpha_{\mathrm{id}_X,A}^{-1} = F_X(\beta_{X,A}) \circ \sigma_{G_{\mathrm{id}_X}(A)} \circ F_X(\beta_{X,A})^{-1} = \sigma_A$$

(we applied the first assumption and the definition of automorphism of a functor). So

$$\pi(\mathrm{id}_X)(\sigma) = (\alpha_{\mathrm{id}_X,A} \circ \sigma_{G_{\mathrm{id}_X}(A)} \circ \alpha_{\mathrm{id}_X,A}^{-1})_{A \in \mathrm{Ob}_{\mathbf{C}_X}} = (\sigma_A)_{A \in \mathrm{Ob}(\mathbf{C}_X)} = \sigma \, .$$

Then $\pi(\mathrm{id}_X) = \mathrm{id}_{\mathrm{Aut}(F_X)} = \mathrm{id}_{\pi(X)}$.
Finally, let X, Y, Z be objects of $\mathbf{D}$ and $f : X \to Y$, $g : Y \to Z$ two morphisms. Let $\sigma = (\sigma_A)_{A \in \mathrm{Ob}(\mathbf{C}_X)}$. For any object C of $\mathbf{C}_Z$, we have that

$$\begin{aligned}
&\alpha_{g,C} \circ \alpha_{f,G_g(C)} \circ \sigma_{G_f(G_g(C))} \circ \alpha_{f,G_g(C)}^{-1} \circ \alpha_{g,C}^{-1} = \\
&\qquad = \alpha_{g\circ f,C} \circ F_X(\gamma_{f,g,C}) \circ \sigma_{G_f(G_g(C))} \circ F_X(\gamma_{f,g,C})^{-1} \circ \alpha_{g\circ f,C}^{-1} = \\
&\qquad\qquad = \alpha_{g\circ f,C} \circ \sigma_{G_{g\circ f}(C)} \circ \alpha_{g\circ f,C}^{-1}
\end{aligned}$$

(we applied the second assumption and the definition of automorphism of a functor). So

$$\begin{aligned}
&\pi(g)(\pi(f)(\sigma)) = \pi(g)\left((\alpha_{f,B} \circ \sigma_{G_f(B)} \circ \alpha_{f,B}^{-1})_{B \in \mathrm{Ob}(\mathbf{C}_Y)}\right) = \\
&\qquad = (\alpha_{g,C} \circ \alpha_{f,G_g(C)} \circ \sigma_{G_f(G_g(C))} \circ \alpha_{f,G_g(C)}^{-1} \circ \alpha_{g,C}^{-1})_{C \in \mathrm{Ob}(\mathbf{C}_Z)} = \\
&\qquad\qquad = (\alpha_{g\circ f,C} \circ \sigma_{G_{g\circ f}(C)} \circ \alpha_{g\circ f,C}^{-1})_{C \in \mathrm{Ob}(\mathbf{C}_Z)} = \pi(g \circ f)(\sigma) \, .
\end{aligned}$$

Then $\pi(g) \circ \pi(f) = \pi(g \circ f)$. Hence π is a functor. □

Chapter 2

Galois theory for schemes

In this chapter we will study the category of finite étale coverings of a connected scheme (we do *not* consider the empty scheme as a connected scheme), with the aim of proving that it is a Galois category (with a suitable fundamental functor). Then the existence of the fundamental group will follow from theorem 1.4.34. In the first section (based on section 4 of [1]), we will deal with the algebraic aspect of our problem: after giving the necessary definitions, we will prove all the algebraic results that will be needed later. In particular, we will define projective separable algebras and we will describe their behaviour under extensions of the scalar ring. The second and third sections follow section 5 of [1]. In our treatment of finite étale coverings, we will point out many analogies with finite coverings of topological spaces. The interested reader can find an extensive discussion of the latter, from the definition to the proof that they form a Galois category if the base space is connected, in the appendix. In the second section, we will define finite étale morphisms and we will study their properties. It will be useful to consider base changes, which will reveal a similarity between finite étale coverings of a scheme and finite coverings of a topological space: the latter are defined as continuous maps which are locally trivial coverings (see the appendix) and in some sense also finite étale coverings are "locally trivial" (but not in the Zariski topology). The analogue of trivial coverings will be the notion of totally split morphisms. In the third section, we will define a functor from the category of finite étale coverings of a scheme X to the category of finite sets and we will prove that this makes the former into a Galois category if X is connected. In the case of topological spaces (see the appendix) we can define a fundamental functor for any point of the space. Similarly, here we will define a fundamental functor for any *geometric point* of our scheme (i.e. any morphism of schemes $\mathrm{Spec}(\Omega) \to X$, where Ω is an algebraically closed field).

2.1 Algebraic preliminaries

We collect in this section all the algebraic results that we will need in the following ones. Rings are always assumed to be commutative with unity and ring homomorphisms preserve the unity. Throughout this section, A will be a ring. We denote by $\mathbf{Mod}_A$ the category of A-modules.

Definition 2.1.1. Let M a finitely generated free A-module, with basis $(w_1, \dots, w_n)$. Let $f : M \to M$ be A-linear. By definition of basis, for any $i = 1, \dots, n$ there exist uniquely determined $a_{i1}, \dots, a_{in} \in A$ such that $f(w_i) = \sum_{j=1}^{n} a_{ij} w_j$. The *trace* of f is defined by

$$\mathrm{Tr}(f) = \sum_{i=1}^{n} a_{ii} \ .$$

Remark 2.1.2. (1) If M is a finitely generated free A-module, then it has a finite basis. Indeed, if $(w_i)_{i \in I}$ is an A-basis of M and $x_1, \dots, x_n$ generate A, then for any $j = 1, \dots, n$ we can write $x_j = \sum_{i \in I_j} a_{ji} w_i$, with I_j a finite subset of I and $a_{ji} \in A$ for any $i \in I_j$. Then M is generated by $(w_i)_{i \in \bigcup_{j=1}^{n} I_j}$. In particular, for any $i_0 \in I$ we have that w_{i_0} is a linear combination of $(w_i)_{i \in \bigcup_{j=1}^{n} I_j}$. But since $(w_i)_{i \in I}$ is a basis, it is a linear independent set. So we must have $i_0 \in \bigcup_{j=1}^{n} I_j$. Then $I = \bigcup_{j=1}^{n} I_j$. This proves that I is finite, because it is a finite union of finite sets. It can also be proved that, if $A \neq 0$, all bases have the same cardinality, which is called the *rank* of M over A and denoted by $\mathrm{rank}_A(M)$ (to prove it, consider any maximal ideal $\mathfrak{m}$ of A and the quotient field $k := A/\mathfrak{m}$, which can be seen as an A-algebra in a natural way: then for any A-basis $(w_1, \dots, w_n)$ of B we have that $(w_1 \otimes 1, \dots, w_n \otimes 1)$ is a k-basis of $M \otimes_A k$, so $n = \dim_k(M \otimes_A k)$ is independent of the choice of the basis).

(2) The trace of an endomorphism, defined as in 2.1.1, is independent of the choice of the basis. The proof is analogous to the well-known one in the case of vector spaces (one proves that the trace of a matrix is invariant by conjugation and that the matrices associated to the same endomorphism with respect to two bases are conjugate to each other).

Lemma 2.1.3. *Let B be an A-algebra. Assume that B is finitely generated and free as an A-module. For every $b \in B$, define $m_b : B \to B$, $x \mapsto bx$. By definition of A-algebra, we have that m_b is A-linear, so we can consider its trace. We define* $\mathrm{Tr}(b) := \mathrm{Tr}(m_b)$.

(1) The map $\mathrm{Tr} : B \to A$, $b \mapsto \mathrm{Tr}(b)$ *is A-linear.*

(2) The map $\varphi : B \to \mathrm{Hom}_A(B, A)$, $x \mapsto (y \mapsto \mathrm{Tr}(xy))$ *is A-linear.*

Proof. (1) Let $(w_1, \dots, w_n)$ be an A-basis of B (see remark 2.1.2). Let $b_1, b_2 \in B$, $\lambda_1, \lambda_2 \in A$. For any $i = 1, \dots, n$, consider $a_{i1}, \dots, a_{in} \in A$ such that $m_{b_1}(w_i) = \sum_{j=1}^{n} a_{ij} w_j$ and $a'_{i1}, \dots, a'_{in} \in A$ such that $m_{b_2}(w_i) = \sum_{j=1}^{n} a'_{ij} w_j$. Then we have

$$\begin{aligned} m_{\lambda_1 b_1 + \lambda_2 b_2}(w_i) &= (\lambda_1 b_1 + \lambda_2 b_2) w_i = \lambda_1 (b_1 w_i) + \lambda_2 (b_2 w_i) = \\ &= \lambda_1 m_{b_1}(w_i) + \lambda_2 m_{b_2}(w_i) = \\ &= \lambda_1 \left(\sum_{j=1}^{n} a_{ij} w_j \right) + \lambda_2 \left(\sum_{j=1}^{n} a'_{ij} w_j \right) = \sum_{j=1}^{n} (\lambda_1 a_{ij} + \lambda_2 a'_{ij}) w_j \ . \end{aligned}$$

So, by definition of trace, we have that

$$\begin{aligned}\operatorname{Tr}(\lambda_1 b_1 + \lambda_2 b_2) = \operatorname{Tr}(m_{\lambda_1 b_1 + \lambda_2 b_2}) = \sum_{i=1}^{n} (\lambda_1 a_{ii} + \lambda_2 a'_{ii}) = \\ = \lambda_1 \left(\sum_{i=1}^{n} a_{ii} \right) + \lambda_2 \left(\sum_{i=1}^{n} a'_{ii} \right) = \\ = \lambda_1 \operatorname{Tr}(m_{b_1}) + \lambda_2 \operatorname{Tr}(m_{b_2}) = \lambda_1 \operatorname{Tr}(b_1) + \lambda_2 \operatorname{Tr}(b_2) \,.\end{aligned}$$

Hence Tr is A-linear.

(2) First of all, we prove that φ is well defined, i.e. that $\varphi(x) : B \to A$ is indeed an A-linear map for any $x \in B$. Let $y_1, y_2 \in B$, $\lambda_1, \lambda_2 \in A$. Then, applying the A-linearity of Tr, we have

$$\begin{aligned}\varphi(x)(\lambda_1 y_1 + \lambda_2 y_2) = \operatorname{Tr}(x(\lambda_1 y_1 + \lambda_2 y_2)) = \operatorname{Tr}(\lambda_1 (x y_1) + \lambda_2 (x y_2)) = \\ = \lambda_1 \operatorname{Tr}(x y_1) + \lambda_2 \operatorname{Tr}(x y_2) = \lambda_1 \varphi(x)(y_1) + \varphi(x)(y_2) \,.\end{aligned}$$

So $\varphi(x)$ is A-linear and φ is well defined.
Let now $x_1, x_2 \in B$, $\lambda_1, \lambda_2 \in A$. Then for any $y \in B$ we have

$$\begin{aligned}\varphi(\lambda_1 x_1 + \lambda_2 x_2)(y) = \operatorname{Tr}((\lambda_1 x_1 + \lambda_2 x_2) y) = \operatorname{Tr}(\lambda_1 (x_1 y) + \lambda_2 (x_2 y)) = \\ = \lambda_1 \operatorname{Tr}(x_1 y) + \lambda_2 \operatorname{Tr}(x_2 y) = \lambda_1 \varphi(x_1)(y) + \lambda_2 \varphi(x_2)(y)\end{aligned}$$

(we applied again the A-linearity of Tr). So $\varphi(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 \varphi(x_1) + \lambda_2 \varphi(x_2)$. Hence φ is A-linear.

□

Definition 2.1.4. Let B be an A-algebra. We say that B is a *free separable A-algebra* if B is finitely generated and free as an A-module and the map φ defined in lemma 2.1.3 is an isomorphism of A-modules.

Remark 2.1.5. Let B be as in lemma 2.1.3. Then $\operatorname{Hom}_A(B, A)$ is always isomorphic to B as an A-module. Indeed, if $(w_1, \ldots, w_n)$ is a basis of B, then $(w_1^*, \ldots, w_n^*)$ is a basis of $\operatorname{Hom}_A(B, A)$, where we defined

$$w_j^* : B \to A, \ \sum_{i=1}^{n} a_i w_i \mapsto a_j$$

for any $j = 1, \ldots, n$. So we have an isomorphism of A-modules $\vartheta : B \to \operatorname{Hom}_A(B, A)$ defined by $\vartheta(w_i) = w_i^*$ for any $i = 1, \ldots, n$ (extended by linearity). This isomorphism, however, depends on the basis.

Example 2.1.6. Consider the A-algebra A^n (with ring operations defined componentwise), which is clearly finitely generated and free as an A-module. We claim that A^n is a free separable A-algebra. Let $(e_1, \ldots, e_n)$ be the canonical basis of A^n, i.e. $e_i = (\delta_{ik})_{k=1,\ldots,n}$ for any $i = 1, \ldots, n$. Let $x = (x_1, \ldots, x_n) \in A^n$. We have that

$$m_x(e_i) = x e_i = (x_1, \ldots, x_n)(\delta_{ik})_{k=1,\ldots,n} = (x_k \delta_{ik})_{k=1,\ldots,n} = x_i e_i$$

for any $i = 1, \dots, n$. Then $\mathrm{Tr}(x) = \mathrm{Tr}(m_x) = \sum_{i=1}^n x_i$. Consider now the map $\varphi : A^n \to \mathrm{Hom}_A(A^n, A)$ defined as in lemma 2.1.3. By what we proved, we have that $\varphi(x)(y) = \mathrm{Tr}(xy) = \mathrm{Tr}((x_1y_1, \dots, x_ny_n)) = \sum_{i=1}^n x_iy_i$ for any $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in A^n$. Define now

$$\psi : \mathrm{Hom}_A(A^n, A) \to A^n,\ f \mapsto (f(e_1), \dots, f(e_n)) \ .$$

For any $x = (x_1, \dots, x_n) \in A^n$, $j \in \{1, \dots, n\}$ we have that $\varphi(x)(e_j) = \sum_{i=1}^n x_i\delta_{ij} = x_j$ and so

$$\psi(\varphi(x)) = (\varphi(x)(e_1), \dots, \varphi(x)(e_n)) = (x_1, \dots, x_n) = x = \mathrm{id}_{A^n}(x) \ .$$

So $\psi \circ \varphi = \mathrm{id}_{A^n}$. Conversely, let $f \in \mathrm{Hom}_A(A^n, A)$ and let $x = (x_1, \dots, x_n) \in A^n$. Then, applying the A-linearity of f, we get that

$$\varphi(\psi(f))(x) = \varphi((f(e_1), \dots, f(e_n)))(x) = \sum_{i=1}^n f(e_i)x_i = f\left(\sum_{i=1}^n x_ie_i\right) = f(x) \ .$$

So $(\varphi \circ \psi)(f) = f = \mathrm{id}_{\mathrm{Hom}_A(A^n,A)}(f)$, for any $f \in \mathrm{Hom}_A(A^n, A)$. Then $\varphi \circ \psi = \mathrm{id}_{\mathrm{Hom}_A(A^n,A)}$. This proves that φ and ψ are inverse to each other. In particular, φ is an isomorphism, i.e. A^n is a free separable A-algebra.

The notion of free separable algebra will be involved in the definition of finite étale morphisms (see 2.2.1). However, in order to prove most results about finite étale morphisms, we will need a more general notion, that of projective separable algebras. To introduce this concept, we start by recalling the definition of projective modules.

Definition 2.1.7. An A-module P is called *projective* if the functor

$$\mathrm{Hom}_A(P, -) : \mathbf{Mod}_A \to \mathbf{Mod}_A$$

is exact, i.e. if for every exact sequence $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ of A-modules the induced sequence $\mathrm{Hom}_A(P, M_0) \xrightarrow{f\circ -} \mathrm{Hom}_A(P, M_1) \xrightarrow{g\circ -} \mathrm{Hom}_A(P, M_2)$ is also exact.

Example 2.1.8. A is a projective A-module, because the functor $\mathrm{Hom}_A(A, -)$ is isomorphic to $\mathrm{id}_{\mathbf{Mod}_A}$.

We prove now some lemmas that will allow us to give a very useful characterization of projective modules.

Lemma 2.1.9. *Let $(P_i)_{i\in I}$ a collection of A-modules and $P := \bigoplus_{i\in I} P_i$. For every A-module M we have an isomorphism*

$$\varphi_M : \mathrm{Hom}_A(P, M) \to \prod_{i\in I} \mathrm{Hom}_A(P_i, M) \ .$$

Moreover, these isomorphisms are compatible, in the sense that, if M, N are A-modules and $f : M \to N$ is an A-linear map, then the following diagram is commutative.

$$\begin{array}{ccc}
\mathrm{Hom}_A(P, M) & \xrightarrow{\varphi_M} & \prod_{i\in I} \mathrm{Hom}_A(P_i, M) \\
{\scriptstyle f\circ -}\big\downarrow & & \big\downarrow{\scriptstyle \prod_{i\in I}(f\circ -)} \\
\mathrm{Hom}_A(P, N) & \xrightarrow{\varphi_N} & \prod_{i\in I} \mathrm{Hom}_A(P_i, N)
\end{array}$$

Proof. For any $j \in J$, define $q_j : P_j \to P,\ x \mapsto (\delta_{ij}x)_{i\in I}$. Notice that, for any $x = (x_i)_{i\in I} \in P$ we have $x = \sum_{i\in I} q_i(x_i)$.
Let M be an A-module. Define

$$\varphi_M : \mathrm{Hom}_A(P, M) \to \prod_{i\in I} \mathrm{Hom}_A(P_i, M),\ h \mapsto (h \circ q_i)_{i\in I}\ .$$

Let $h_1, h_2 \in \mathrm{Hom}_A(P, M)$, $\lambda_1, \lambda_2 \in A$. Then

$$\varphi(\lambda_1 h_1 + \lambda_2 h_2) = ((\lambda_1 h_1 + \lambda_2 h_2) \circ q_i)_{i\in I} = (\lambda_1(h_1 \circ q_i) + \lambda_2(h_2 \circ q_i))_{i\in I} = \\ = \lambda_1(h_1 \circ q_i)_{i\in I} + \lambda_2(h_2 \circ q_i)_{i\in I} = \lambda_1\varphi(h_1) + \lambda_2\varphi(h_2)\ .$$

So φ_M is A-linear. Conversely, if $(h_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_A(P_i, M)$, we can define $h : P \to M,\ (x_i)_{i\in I} \mapsto \sum_{i\in I} h_i(x_i)$ (notice that this sum is well defined because only finitely many of the x_i's are non-zero). If $(x_i)_{i\in I}, (y_i)_{i\in I} \in P$, $\lambda_1, \lambda_2 \in A$, then we have

$$h\left(\lambda_1(x_i)_{i\in I} + \lambda_2(y_i)_{i\in I}\right) = h\left((\lambda_1 x_i + \lambda_2 y_i)_{i\in I}\right) = \\ = \sum_{i\in I} h_i(\lambda_1 x_i + \lambda_2 y_i) = \sum_{i\in I}(\lambda_1 h_i(x_i) + \lambda_2 h_i(y_i)) = \\ = \lambda_1 \sum_{i\in I} h_i(x_i) + \lambda_2 \sum_{i\in I} h_i(y_i) = \lambda_1 h\left((x_i)_{i\in I}\right) + \lambda_2 h\left((y_i)_{i\in I}\right)\ ,$$

because each h_i is A-linear. So h is A-linear. Then we can define

$$\varphi'_M : \prod_{i\in I} \mathrm{Hom}_A(P_i, M) \to \mathrm{Hom}_A(P, M), \\ (h_i)_{i\in I} \mapsto \left(h : P \to M,\ (x_i)_{i\in I} \mapsto \sum_{i\in I} h_i(x_i)\right)\ .$$

Let $(g_i)_{i\in I}, (h_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_A(P_i, M)$, $\lambda_1, \lambda_2 \in A$. For any $(x_i)_{i\in I} \in P$, we have

$$\varphi'_M\left(\lambda_1(g_i)_{i\in I} + \lambda_2(h_i)_{i\in I}\right)\left((x_i)_{i\in I}\right) = \varphi'_M\left((\lambda_1 g_i + \lambda_2 h_i)_{i\in I}\right)\left((x_i)_{i\in I}\right) = \\ = \sum_{i\in I}(\lambda_1 g_i + \lambda_2 h_i)(x_i) = \sum_{i\in I}(\lambda_1 g_i(x_i) + \lambda_2 h_i(x_i)) = \lambda_1 \sum_{i\in I} g_i(x_i) + \lambda_2 \sum_{i\in I} h_i(x_i) = \\ = \lambda_1\varphi'_M\left((g_i)_{i\in I}\right)\left((x_i)_{i\in I}\right) + \lambda_2\varphi'_M\left((h_i)_{i\in I}\right)\left((x_i)_{i\in I}\right)\ .$$

So $\varphi'_M\left(\lambda_1(g_i)_{i\in I} + \lambda_2(h_i)_{i\in I}\right) = \lambda_1\varphi'_M\left((g_i)_{i\in I}\right) + \lambda_2\varphi'_M\left((h_i)_{i\in I}\right)$ and φ'_M is A-linear. We check that φ_M and φ'_M are inverse to each other. Let $h \in \mathrm{Hom}_A(P, M)$. For any $x = (x_i)_{i\in I} \in P$ we have that

$$\varphi'_M(\varphi_M(h))(x)\varphi'_M\left((h \circ q_i)_{i\in I}\right)\left((x_i)_{i\in I}\right) = \sum_{i\in I} h(q_i(x_i)) = h\left(\sum_{i\in I} q_i(x_i)\right) = h(x)\ .$$

So $\varphi'_M \circ \varphi_M = \mathrm{id}_{\mathrm{Hom}_A(P,M)}$. Let now $(h_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_A(P_i, M)$ and define $h = \varphi'_M\left((h_i)_{i\in I}\right)$. For any $j \in I$, $x \in P_j$, we have

$$h(q_j(x)) = h\left((\delta_{ij}x)_{i\in I}\right) = \sum_{i\in I} h_i(\delta_{ij}x) = \sum_{i\in I} \delta_{ij} h_i(x) = h_j(x)$$

and so $h \circ q_j = h_j$. Then we have that

$$\varphi_M\left(\varphi'_M\left((h_{i\in I})\right)\right) = \varphi_M(h) = (h \circ q_i)_{i\in I} = (h_i)_{i\in I} = \mathrm{id}_{\prod_{i\in I}\mathrm{Hom}_A(P_i,M)}\left((h_i)_{i\in I}\right) .$$

So $\varphi_M \circ \varphi'_M = \mathrm{id}_{\prod_{i\in I}\mathrm{Hom}_A(P_i,M)}$. Then φ_M and φ'_M are inverse to each other.
Finally, let M, N be A-modules and $f : M \to N$ an A-linear map. For any $h \in \mathrm{Hom}_A(P, M)$ we have that

$$\varphi_N(f \circ h) = (f \circ h \circ q_i)_{i\in I} = \left(\prod_{i\in I}(f \circ -)\right)\left((h \circ q_i)_{i\in I}\right) = \left(\prod_{i\in I}(f \circ -)\right)\left(\varphi_M(h)\right) .$$

This proves the commutativity of the diagram. □

Corollary 2.1.10. *Let $(P_i)_{i\in I}$ a collection of A-modules and define $P := \bigoplus_{i\in I} P_i$. Then P is projective if and only if each P_i is projective.*

Proof. For any $i \in I$, denote $f^i_* : \mathrm{Hom}_A(P_i, M_0) \to \mathrm{Hom}_A(P_i, M_1),\ h \mapsto f \circ h$ and $g^i_* : \mathrm{Hom}_A(P_i, M_1) \to \mathrm{Hom}_A(P_i, M_2),\ h \mapsto g \circ h$.
Let $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ be an exact sequence of A-modules. By lemma 2.1.9, there is an isomorphism of sequences between

$$\mathrm{Hom}_A(P, M_0) \xrightarrow{f\circ -} \mathrm{Hom}_A(P, M_1) \xrightarrow{g\circ -} \mathrm{Hom}_A(P, M_2)$$

and

$$\prod_{i\in I}\mathrm{Hom}_A(P_i, M_0) \xrightarrow{\prod_{i\in I} f^i_*} \prod_{i\in I}\mathrm{Hom}_A(P_i, M_1) \xrightarrow{\prod_{i\in I} g^i_*} \prod_{i\in I}\mathrm{Hom}_A(P_i, M_2) .$$

So P is projective if and only if the last sequence is exact for every exact sequence $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$.We have that

$$\mathrm{Ker}\left(\prod_{i\in I} g^i_*\right) = \left\{(h_i)_{i\in I} \in \prod_{i\in I}\mathrm{Hom}_A(P_i, M_1)\ \middle|\ (g \circ h_i)_{i\in I} = (0)_{i\in I}\right\} =$$

$$= \left\{(h_i)_{i\in I} \in \prod_{i\in I}\mathrm{Hom}_A(P_i, M_1)\ \middle|\ \forall i \in I \quad g \circ h_i = 0\right\} = \prod_{i\in I}\mathrm{Ker}(g^i_*)$$

and

$$\mathrm{Im}\left(\prod_{i\in I} f^i_*\right) = \left\{(h_i)_{i\in I} \in \prod_{i\in I}\mathrm{Hom}_A(P_i, M_1)\ \middle|\ \exists (h'_i)_{i\in I} \in \prod_{i\in I}\mathrm{Hom}_A(P_i, M_0) : (h_i)_{i\in I} = (f \circ h'_i)_{i\in I}\right\} =$$

$$= \left\{(h_i)_{i\in I} \in \prod_{i\in I}\mathrm{Hom}_A(P_i, M_1)\ \middle|\ \forall i \in I\ \exists h'_i \in \mathrm{Hom}_A(P_i, M_0) : h_i = g \circ h'_i\right\} =$$

$$= \prod_{i\in I}\mathrm{Im}(f^i_*) .$$

Then we have that $\operatorname{Ker}\left(\prod_{i\in I} g_*^i\right) = \operatorname{Im}\left(\prod_{i\in I} f_*^i\right)$ if and only if $\operatorname{Ker}(g_*^i) = \operatorname{Im}(f_*^i)$ for every $i \in I$. This means that the sequence

$$\prod_{i\in I} \operatorname{Hom}_A(P_i, M_0) \xrightarrow{\prod_{i\in I} f_*^i} \prod_{i\in I} \operatorname{Hom}_A(P_i, M_1) \xrightarrow{\prod_{i\in I} g_*^i} \prod_{i\in I} \operatorname{Hom}_A(P_i, M_2)$$

is exact if and only if each of the sequences

$$\operatorname{Hom}_A(P_i, M_0) \xrightarrow{f_*^i} \operatorname{Hom}_A(P_i, M_1) \xrightarrow{g_*^i} \operatorname{Hom}_A(P_i, M_2)$$

is exact. Since this holds for every exact sequence $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ of A-modules, we have that P is projective if and only if each P_i is projective. ☐

Example 2.1.11. Any free A-module is projective. Indeed, if an A-module is free then it is isomorphic to $\bigoplus_{i\in I} A$ for some index set I. So it is projective by corollary 2.1.10 and example 2.1.8.

Definition 2.1.12. A short exact sequence of A-modules $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0$ is said to *split* if there is an isomorphism of A-modules $\varphi : M_1 \to M_0 \oplus M_2$ such that $\varphi \circ f = i_0$ and $g \circ \varphi^{-1} = p_2$, where we defined $i_0 : M_0 \to M_0 \oplus M_2,\ x \mapsto (x, 0)$ and $p_2 : M_0 \oplus M_2 \to M_2,\ (x, y) \mapsto y$. The definition is illustrated by the following diagram.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_0 & \xrightarrow{f} & M_1 & \xrightarrow{g} & M_2 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_{M_0}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_{M_2}} & & \\
0 & \longrightarrow & M_0 & \xrightarrow[i_0]{} & M_0 \oplus M_2 & \xrightarrow[p_2]{} & M_2 & \longrightarrow & 0
\end{array}$$

Lemma 2.1.13. *Let $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0$ be a short exact sequence of A-modules. The following are equivalent:*

(i) the sequence splits;

(ii) there exists an A-linear map $\alpha : M_1 \to M_0$ such that $\alpha \circ f = \mathrm{id}_{M_0}$;

(iii) there exists an A-linear map $\beta : M_2 \to M_1$ such that $g \circ \beta = \mathrm{id}_{M_1}$.

Proof. Define $i_0 : M_0 \to M_0 \oplus M_2,\ x \mapsto (x, 0)$, $i_2 : M_2 \to M_0 \oplus M_2,\ y \mapsto (0, y)$, $p_1 : M_0 \oplus M_2 \to M_0,\ (x, y) \mapsto x$ and $p_2 : M_0 \oplus M_2 \to M_2,\ (x, y) \mapsto y$. It is clear that these maps are A-linear. Moreover, notice that $p_0 \circ i_0 = \mathrm{id}_{M_0}$ and $p_2 \circ i_2 = \mathrm{id}_{M_2}$.

(i) $\Longrightarrow$ (ii) Since the sequence $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0$ splits, there exists an isomorphism of A-modules $\varphi : M_1 \to M_0 \oplus M_2$ such that $\varphi \circ f = i_0$ and $g \circ \varphi^{-1} = p_2$. Define $\alpha := p_0 \circ \varphi : M_1 \to M_0$. Then α is A-linear, because it is the composition of A-linear maps, and we have $\alpha \circ f = p_0 \circ \varphi \circ f = p_0 \circ i_0 = \mathrm{id}_{M_0}$.

(ii) $\Longrightarrow$ (i) Define $\varphi : M_1 \to M_0 \oplus M_2,\ x \mapsto (\alpha(x), g(x))$. We have that φ is A-linear, because α and g are A-linear. We claim that φ is bijective. Let $(y_0, y_2) \in M_0 \oplus M_2$. We have that g is surjective, by definition of short exact sequence. So there exists $x_1 \in M_1$ such that $y_2 = g(x_1)$. Consider $x_2 = f(y_0 - \alpha(x_1)) \in \operatorname{Im}(f) \subseteq M_1$. By definition of exact sequence, we have that $\operatorname{Im}(f) = \operatorname{Ker}(g)$. So $g(x_2) = 0$. Then we have that $g(x_1+x_2) = g(x_1)+g(x_2) = y_2$. Moreover, since $\alpha \circ f = \mathrm{id}_{M_0}$, we have that $\alpha(x_1 + x_2) = \alpha(x_1) + \alpha(x_2) = \alpha(x_1) + (\alpha \circ f)(y_0 - \alpha(x_1)) = \alpha(x_1) + y_0 - \alpha(x_1) = y_0$. Then $\varphi(x_1 + x_2) = (y_0, y_2)$. This proves that φ is surjective. Let $x \in \operatorname{Ker}(\varphi)$, i.e. $(\alpha(x), g(x)) = \varphi(x) = (0, 0)$. Then $\alpha(x) = 0$ and $g(x) = 0$. So $x \in \operatorname{Ker}(g)$. But $\operatorname{Ker}(g) = \operatorname{Im}(f)$, by definition of exact sequence. So there exists $m \in M_0$ such that $x = f(m)$. Then $0 = \alpha(x) = \alpha(f(m)) = m$, because $\alpha \circ f = \mathrm{id}_{M_0}$. This implies that $x = f(0) = 0$ and so φ is injective. Then φ is an isomorphism of A-modules. For any $x \in M_0$, we have that $(\varphi \circ f)(x) = \varphi(f(x)) = (\alpha(f(x)), g(f(x))) = (x, 0) = i_0(x)$, because $\alpha \circ f = \mathrm{id}_{M_0}$ and $g \circ f = 0$ (definition of exact sequence). So $\varphi \circ f = i_0$. On the other hand, for any $x \in M_1$ we have that $(p_2 \circ \varphi)(x) = p_2((\alpha(x), g(x))) = g(x)$. So $p_2 \circ \varphi = g$, i.e. $g \circ \varphi^{-1} = p_2$. This proves that the sequence $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0$ splits.

(i) $\Longrightarrow$ (iii) Since the sequence $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0$ splits, there exists an isomorphism of A-modules $\varphi : M_1 \to M_0 \oplus M_2$ such that $\varphi \circ f = i_0$ and $g \circ \varphi^{-1} = p_2$. Define $\beta := \varphi^{-1} \circ i_2 : M_2 \to M_1$. Then β is A-linear, because it is the composition of A-linear maps, and we have $g \circ \beta = g \circ \varphi^{-1} \circ i_2 = p_2 \circ i_2 = \mathrm{id}_{M_2}$.

(iii) $\Longrightarrow$ (i) Define $\psi : M_0 \oplus M_2 \to M_1,\ (x, y) \mapsto f(x) + \beta(y)$. Since f and β are A-linear, for any $(x_1, y_1), (x_2, y_2) \in M_0 \oplus M_2$, $\lambda_1, \lambda_2 \in A$ we have

$$\begin{aligned} &\psi(\lambda_1(x_1, y_1) + \lambda_2(x_2, y_2)) = \psi((\lambda_1 x_1 + \lambda_2 x_2, \lambda_1 y_1 + \lambda_2 y_2)) = \\ &= f(\lambda_1 x_1 + \lambda_2 x_2) + \beta(\lambda_1 y_1 + \lambda_2 y_2) = \lambda_1 f(x_1) + \lambda_2 f(x_2) + \lambda_1 \beta(y_1) + \lambda_2 \beta(y_2) = \\ &= \lambda_1(f(x_1) + \beta(y_1)) + \lambda_2(f(x_2) + \beta(y_2)) = \lambda_1 \psi((x_1, y_1)) + \lambda_2 \psi((x_2, y_2)) \,. \end{aligned}$$

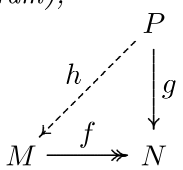
So ψ is A-linear. We claim that ψ is bijective. Let $m \in M_1$. Since $g \circ \beta = \mathrm{id}_{M_2}$, we have that $g(\beta(g(m))) = g(m)$. So $g(m - \beta(g(m))) = g(m) - g(\beta(g(m))) = 0$, i.e. $m - \beta(g(m)) \in \operatorname{Ker}(g)$. By definition of exact sequence, we have that $\operatorname{Ker}(g) = \operatorname{Im}(f)$. So there exists $x \in M_0$ such that $m - \beta(g(m)) = f(x)$. Then $\psi((x, g(m))) = f(x) + \beta(g(m)) = m - \beta(g(m)) + \beta(g(m)) = m$. This proves that ψ is surjective. Let $(x, y) \in \operatorname{Ker}(\psi)$, i.e. $f(x) + \beta(y) = \psi((x, y)) = 0$. Then $\beta(y) = -f(x) = f(-x) \in \operatorname{Im}(f)$. By definition of exact sequence, we have that $\operatorname{Im}(f) = \operatorname{Ker}(g)$. So $g(\beta(y)) = 0$. Since $g \circ \beta = \mathrm{id}_{M_2}$, we have that $y = g(\beta(y)) = 0$. Then $f(x) = -\beta(y) = -\beta(0) = 0$. But f is injective by definition of short exact sequence, so we must have $x = 0$. Then $(x, y) = (0, 0)$ and so ψ is injective. Then ψ is an isomorphism of A-modules. Define $\varphi := \psi^{-1} : M_1 \to M_0 \oplus M_2$. For any $x \in M_0$, we have that $(\psi \circ i_0)(x) = \psi((x, 0)) = f(x) + \beta(0) = f(x)$. So $\psi \circ i_0 = f$, which implies that $\varphi \circ f = \psi^{-1} \circ f = i_0$. On the other hand, for any $(x, y) \in M_0 \oplus M_2$ we have that $(g \circ \psi)((x,y)) = g(f(x) + \beta(y)) = g(f(x)) + g(\beta(y)) = y = p_2((x,y))$, because $g \circ f = 0$ (by definition of exact sequence) and $g \circ \beta = \mathrm{id}_{M_2}$. So $g \circ \varphi^{-1} = g \circ \psi = p_2$. This proves that the sequence $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0$ splits.

□

Lemma 2.1.14. *Let P be an A-module. The following are equivalent:*

(i) P is projective;

(ii) for every A-modules M, N, every surjective A-linear map $f : M \to N$ and every A-linear map $g : P \to N$ there exists an A-linear map $h : P \to M$ such that $f \circ h = g$ (see also the diagram);



(iii) every short exact sequence of A-modules $0 \to M_0 \to M_1 \to P \to 0$ splits;

(iv) there exists an A-module Q such that $P \oplus Q$ is a free A-module.

Proof. (i) $\Longrightarrow$ (ii) Let M, N be A-modules, $f \in \mathrm{Hom}_A(M,N)$ surjective and $g \in \mathrm{Hom}_A(P,N)$. Since f is surjective, the sequence $M \xrightarrow{f} N \to 0$ is exact. Then, since P is projective, the sequence

$$\mathrm{Hom}_A(P,M) \xrightarrow{f\circ -} \mathrm{Hom}_A(P,N) \to 0$$

is also exact. This means that the map

$$f_* : \mathrm{Hom}_A(P,M) \to \mathrm{Hom}_A(P,N),\ h \mapsto f \circ h$$

is surjective. Then there exists $h \in \mathrm{Hom}_A(P,M)$ such that $g = f_*(h) = f \circ h$.

(ii) $\Longrightarrow$ (iii) Let $0 \to M_0 \to M_1 \xrightarrow{f} P \to 0$ be a short exact sequence. Then $f : M_1 \to P$ is surjective. Consider $g := \mathrm{id}_P \in \mathrm{Hom}_A(P,P)$. Then we can apply the assumption and get an A-linear map $h : P \to M_1$ such that $f \circ h = g = \mathrm{id}_P$. By lemma 2.1.13, this implies that the sequence $0 \to M_0 \to M_1 \to P \to 0$ splits.

(iii) $\Longrightarrow$ (iv) Let $(w_i)_{i\in I}$ be a set of generators for P over A. Consider the free module $F = \bigoplus_{i\in I} A$, with basis $(e_i)_{i\in I}$. Then we can define an A-linear map $f : F \to P$ by $f(e_i) = w_i$ for any $i \in I$ (extended by linearity). Let $Q := \mathrm{Ker}(f) \subseteq F$ and denote by $i : Q \to F$ the inclusion, which is clearly A-linear. Then the sequence $0 \to Q \xrightarrow{i} F \xrightarrow{f} P \to 0$ is exact. By assumption, it splits. So we have that $P \oplus Q \cong F$ is free.

(iv) $\Longrightarrow$ (i) This follows immediately from 2.1.10 and 2.1.11.

□

Corollary 2.1.15. *Let P be a finitely projective A-module. Then P is projective if and only if there exist an A-module Q and an $n \in \mathbb{N}$ such that $P \oplus Q \cong A^n$.*

Proof. If there exist an A-module Q and an $n \in \mathbb{N}$ such that $P \oplus Q \cong A^n$, then P is projective by the implication (iv) $\implies$ (i) in the lemma 2.1.14. Conversely, assume that P is projective. Let $(w_1, \dots, w_n)$ be a set of generators of P over A and define an A-linear map $\varphi : A^n \to P$ by $\varphi(e_i) = w_i$, extended by linearity (where $(e_1, \dots, e_n)$ is the canonical basis of A^n). Then the sequence

$$0 \to \mathrm{Ker}(\varphi) \xrightarrow{i} A^n \xrightarrow{\varphi} P \to 0$$

is exact (where $i : \mathrm{Ker}(\varphi) \to A^n$ is the canonical inclusion). Since P is projective, this sequence splits, by lemma 2.1.14 ((i) $\implies$ (iii)). Then $P \oplus \mathrm{Ker}(\varphi) \cong A^n$. □

Related to the notion of projective A-module is that of flat A-module.

Definition 2.1.16. Let M be an A-module.

(1) We say that P is *flat* if the functor

$$P \otimes - : \mathbf{Mod}_A \to \mathbf{Mod}_A$$

is exact, i.e. if for every exact sequence $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ of A-modules the induced sequence $P \otimes M_0 \xrightarrow{\mathrm{id}_P \otimes f} P \otimes M_1 \xrightarrow{\mathrm{id}_P \otimes g} P \otimes M_2$ is also exact.

(2) We say that M is *faithfully flat* if a sequence $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ of A-modules is exact if and only if the induced sequence $P \otimes M_0 \xrightarrow{\mathrm{id}_P \otimes f} P \otimes M_1 \xrightarrow{\mathrm{id}_P \otimes g} P \otimes M_2$ is exact.

Remark 2.1.17. From the definitions it is clear that any faithfully flat A-module is also flat.

Example 2.1.18. A is a faithfully flat (in particular, flat) A-module, because the functor $A \otimes -$ is isomorphic to $\mathrm{id}_{\mathbf{Mod}_A}$.

The following resuls are the analogue of lemma 2.1.9 and corollary 2.1.10.

Lemma 2.1.19. *Let $(P_i)_{i \in I}$ a collection of A-modules and $P := \bigoplus_{i \in I} P_i$. For every A-module M we have an isomorphism*

$$\psi_M : P \otimes_A M \to \bigoplus_{i \in I} (P_i \otimes_A M) .$$

Moreover, these isomorphisms are compatible, in the sense that, if M, N are A-modules and $f : M \to N$ is an A-linear map, then the following diagram is commutative.

$$\begin{array}{ccc} P \otimes_A M & \xrightarrow{\psi_M} & \bigoplus_{i \in I}(P_i \otimes_A M) \\ {\scriptstyle \mathrm{id}_P \otimes f} \downarrow & & \downarrow {\scriptstyle \bigoplus_{i \in I}(\mathrm{id}_{P_i} \otimes f)} \\ P \otimes_A N & \xrightarrow{\psi_N} & \bigoplus_{i \in I}(P_i \otimes_A N) \end{array}$$

Proof. For any $j \in J$, define $q_j : P_j \to P$, $x \mapsto (\delta_{ij}x)_{i\in I}$. Notice that, for any $x = (x_i)_{i\in I} \in P$ we have $x = \sum_{i\in I} q_i(x_i)$.
Let M be an A-module. We define

$$\psi_M : P \otimes_A M \to \bigoplus_{i\in I}(P_i \otimes_A M),\ (x_i)_{i\in I} \otimes m \mapsto (x_i \otimes m)_{i\in I}\ ,$$

extended by linearity (we can do so because the map $P \times M \to \bigoplus_{i\in I}(P_i \otimes_A M)$, $((x_i)_{i\in I}, m) \mapsto (x_i \otimes m)_{i\in I}$ is A-bilinear). So ψ_M is an A-linear map. Conversely, for any $j \in I$ we can define

$$\psi'_{M,j} : P_j \otimes_A M \to P \otimes_A M,\ x \otimes m \mapsto q_j(x) \otimes m\ ,$$

extended by linearity (we can do so because the map $P_j \times M \to P \otimes_A M)$, $(x.m) \mapsto q_j(x) \otimes m$ is A-bilinear). Then we define

$$\psi'_M : \bigoplus_{i\in I}(P_i \otimes_A M) \to P \otimes_A M,\ (x_i)_{i\in I} \mapsto \sum_{i\in I} \psi'_{M,i}(x_i)\ ,$$

which is A-linear, because $\psi'_M = \varphi'_{P\otimes_A M}\left((\psi'_{M,i})_{i\in I}\right)$, where

$$\varphi'_{P\otimes_A M} : \prod_{i\in I} \mathrm{Hom}_A(P_i \otimes_A M, P \otimes_A M) \to \mathrm{Hom}_A\left(\bigoplus_{i\in I}(P_i \otimes_A M), P \otimes_A M\right)$$

is defined as in lemma 2.1.9). We check that ψ_M and ψ'_M are inverse to each other. Let $(x_i)_{i\in I} \otimes m \in P \otimes_A M$. Then

$$\psi'_M\left(\psi_M\left((x_i)_{i\in I} \otimes m\right)\right) = \psi'_M\left((x_i \otimes m)_{i\in I}\right) = \sum_{i\in I} \psi'_{M,i}(x_i \otimes m) =$$
$$= \sum_{i\in I}(q_i(x_i) \otimes m) = \left(\sum_{i\in I} q_i(x_i)\right) \otimes m = x \otimes m = \mathrm{id}_{P\otimes_A M}(x \otimes m)\ .$$

Then $\psi'_M \circ \psi_M = \mathrm{id}_{P\otimes_A M}$ (by linearity, it is enough to check equality on pure tensors). Let now $(x_i \otimes m_i)_{i\in I} \in \bigoplus_{i\in I}(P_i \otimes_A M)$. Then we have

$$\psi_M\left(\psi'_M\left((x_i \otimes m_i)_{i\in I}\right)\right) = \psi_M\left(\sum_{i\in I} \psi'_{M,i}(x_i \otimes m_i)\right) = \psi_M\left(\sum_{i\in I} q_i(x_i) \otimes m_i\right) =$$
$$= \sum_{i\in I} \psi_M(q_i(x_i) \otimes m_i) = \sum_{j\in I} \psi_M((\delta_{ij}x_j)_{i\in I} \otimes m_j) = \sum_{j\in I}\left((\delta_{ij}x_j \otimes m_j)_{i\in I}\right) =$$
$$\left(\sum_{j\in I}(\delta_{ij}x_j \otimes m_j)\right)_{i\in I} = (x_i \otimes m_i)_{i\in I} = \mathrm{id}_{\bigoplus_{i\in I}(P_i\otimes_A M)}\left((x_i \otimes m_i)_{i\in I}\right)\ .$$

So $\psi_M \circ \psi'_M = \mathrm{id}_{\bigoplus_{i\in I}(P_i\otimes_A M)}$ (also here, by linearity it is enough to check equality on a set of generators). Then ψ_M and ψ'_M are inverse to each other.

Finally, let M, N be A-modules and $f : M \to N$ an A-linear map. For any $(x_i)_{i\in I} \otimes m \in P \otimes_A M$, we have that

$$\psi_N \left((\mathrm{id}_P \otimes f) \left((x_i)_{i\in I} \otimes m \right) \right) = \psi_N \left((x_i)_{i\in I} \otimes f(m) \right) = (x_i \otimes f(m))_{i\in I} = \\ = \left(\bigoplus_{i\in I} (\mathrm{id}_{P_i} \otimes f) \right) \left((x_i \otimes m)_{i\in I} \right) = \left(\bigoplus_{i\in I} (\mathrm{id}_{P_i} \otimes f) \right) \left(\psi_M \left((x_i)_{i\in I} \otimes m \right) \right) .$$

So $\psi_N \circ (\mathrm{id}_P \otimes f) = \left(\bigoplus_{i\in I} (\mathrm{id}_{P_i} \otimes f) \right) \circ \psi_M$ (by linearity, it is enough to check equality on pure tensors), as we wanted. □

Corollary 2.1.20. *Let $(P_i)_{i\in I}$ a collection of A-modules and define $P := \bigoplus_{i\in I} P_i$. Then P is flat if and only if each P_i is flat.*

Proof. Let $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ be an exact sequence of A-modules. By lemma 2.1.19, there is an isomorphism of sequences between

$$P \otimes_A M_0 \xrightarrow{\mathrm{id}_P \otimes f} P \otimes_A M_1 \xrightarrow{\mathrm{id}_P \otimes g} P \otimes_A M_2$$

and

$$\bigoplus_{i\in I} (P_i \otimes_A M_0) \xrightarrow{\bigoplus_{i\in I} (\mathrm{id}_{P_i} \otimes f)} \bigoplus_{i\in I} (P_i \otimes_A M_1) \xrightarrow{\bigoplus_{i\in I} (\mathrm{id}_{P_i} \otimes g)} \bigoplus_{i\in I} (P_i \otimes_A M_2) .$$

So P is flat if and only if the last sequence is exact for every exact sequence $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$.We have that

$$\mathrm{Ker} \left(\bigoplus_{i\in I} (\mathrm{id}_{P_i} \otimes g) \right) = \\ = \left\{ (x_i)_{i\in I} \in \bigoplus_{i\in I} (P_i \otimes_A M_1) \;\middle|\; ((\mathrm{id}_{P_i} \otimes g)(x_i))_{i\in I} = (0)_{i\in I} \right\} = \\ = \left\{ (x_i)_{i\in I} \in \bigoplus_{i\in I} (P_i \otimes_A M_1) \;\middle|\; \forall i \in I \quad (\mathrm{id}_{P_i} \otimes g)(x_i) = 0 \right\} = \bigoplus_{i\in I} \mathrm{Ker}(\mathrm{id}_{P_i} \otimes g)$$

and

$$\mathrm{Im} \left(\bigoplus_{i\in I} (\mathrm{id}_{P_i} \otimes f) \right) = \left\{ (x_i)_{i\in I} \in \bigoplus_{i\in I} (P_i \otimes_A M_1) \;\middle|\; \exists (x_i')_{i\in I} \in \bigoplus_{i\in I} (P_i \otimes_A M_0) : \right. \\ \left. (x_i)_{i\in I} = ((\mathrm{id}_{P_i} \otimes f)(x_i'))_{i\in I} \right\} = \\ = \left\{ (x_i)_{i\in I} \in \bigoplus_{i\in I} (P_i \otimes_A M_1) \;\middle|\; \forall i \in I \; \exists x_i' \in P_i \otimes_A M_0 : x_i = (\mathrm{id}_{P_i} \otimes f)(x_i') \right\} = \\ = \bigoplus_{i\in I} \mathrm{Im}(\mathrm{id}_{P_i} \otimes f) .$$

Then $\operatorname{Ker}\left(\bigoplus_{i\in I}(\mathrm{id}_{P_i}\otimes g)\right) = \operatorname{Im}\left(\bigoplus_{i\in I}(\mathrm{id}_{P_i}\otimes f)\right)$ if and only if $\operatorname{Ker}(\mathrm{id}_{P_i}\otimes g) = \operatorname{Im}(\mathrm{id}_{P_i}\otimes f)$ for every $i \in I$. This means that the sequence

$$\bigoplus_{i\in I}(P_i \otimes_A M_0) \xrightarrow{\bigoplus_{i\in I}(\mathrm{id}_{P_i}\otimes f)} \bigoplus_{i\in I}(P_i \otimes_A M_1) \xrightarrow{\bigoplus_{i\in I}(\mathrm{id}_{P_i}\otimes g)} \bigoplus_{i\in I}(P_i \otimes_A M_2)$$

is exact if and only if each of the sequences

$$P_i \otimes_A M_0 \xrightarrow{\mathrm{id}_{P_i}\otimes f} P_i \otimes_A M_1 \xrightarrow{\mathrm{id}_{P_i}\otimes g} P_i \otimes_A M_2$$

is exact. Since this holds for every exact sequence $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ of A-modules, we have that P is flat if and only if each P_i is flat. □

Example 2.1.21. Any free A-module is flat. Indeed, if an A-module is free then it is isomorphic to $\bigoplus_{i\in I} A$ for some index set I. So it is flat by corollary 2.1.20 and example 2.1.18.

Corollary 2.1.22. *Any projective A-module is flat.*

Proof. Let P be a projective A-module. By lemma 2.1.14 ((i) $\Longrightarrow$ (iv)), there exists an A-module Q such that $P \oplus Q$ is free. Then $P \oplus Q$ is flat by example 2.1.21. By corollary 2.1.20, this implies that P is flat. □

We want to give now a local characterization of finitely generated projective A-modules. We start with the case when A is local and then we will reduce to this case through localization.

Lemma 2.1.23. *Assume that A is local. Then a finitely generated A-module is projective if and only if it is free.*

Proof. Let $\mathfrak{m}$ be the unique maximal ideal of A and $k := A/\mathfrak{m}$ the residue field. For any $a \in A$, denote by $\overline{a}$ the image of a through the canonical projection $A \to A/\mathfrak{m}$. We already know that any free A-module is projective (example 2.1.11). Conversely, assume that P is a finitely generated projective module and consider $P/\mathfrak{m}P$ as a k-module in the obvious way. For any $x \in P$, denote by $\overline{x}$ the image of x through the canonical projection $P \to P/\mathfrak{m}P$. Let $(w_1, \dots, w_n)$ be a set of generators of P over A. Then $(\overline{w_1}, \dots, \overline{w_n})$ generates $P/\mathfrak{m}P$ over A and so also over $A/\mathfrak{m} = k$. By the well-known properties of vector spaces, there exists a subset $I \subseteq \{1, \dots, n\}$ such that $(\overline{w_i})_{i\in I}$ is a k-basis of $P/\mathfrak{m}P$. Consider the free module $F := \bigoplus_{i\in I} A$, with basis $(e_i)_{i\in I}$, and define an A-linear map $f : F \to P$ by $\varphi(e_i) = w_i$ for any $i \in I$ (extended by linearity). First of all, we prove that f is surjective. Consider the k-module $F/\mathfrak{m}F$ and, for any $x \in F$, denote by $\overline{x}$ the image of x through the canonical projection $F \to F/\mathfrak{m}F$. Since $(e_i)_{i\in I}$ generates F over A, we have that $(\overline{e_i})_{i\in I}$ generates $F/\mathfrak{m}F$ over A and so also over $A/\mathfrak{m} = k$. Moreover, if $\sum_{i\in I} \lambda_i \overline{e_i} = 0$, with $\lambda_i \in k$ for any $i \in I$, then for any $i \in I$ there exists $a_i \in I$ such that $\lambda_i = \overline{a_i}$ and so we have

$$0 = \sum_{i\in I} \lambda_i \overline{e_i} = \sum_{i\in I} \overline{a_i}\, \overline{e_i} = \overline{\sum_{i\in I} a_i e_i}\ ,$$

which means that $\sum_{i\in I} a_i e_i \in \mathfrak{m}F$. Then there exist $b_1,\dots,b_m \in \mathfrak{m}$, $x_1,\dots,x_m \in F$ ($m \in \mathbb{N}$) such that $\sum_{i\in I} a_i e_i = \sum_{j=1}^m b_j x_j$. For any $j = 1,\dots,m$, we can write $x_j = \sum_{i\in I} c_{ji} e_i$, with $c_{ji} \in A$ for any $i \in I$. Then we have

$$\sum_{i\in I} a_i e_i = \sum_{j=1}^m b_j \left(\sum_{i\in I} c_{ji} e_i\right) = \sum_{i\in I}\left(\sum_{j=1}^m b_j c_{ji}\right) e_i \ .$$

Since $(e_i)_{i\in I}$ is a basis of F, we must have $a_i = \sum_{j=1}^m b_j c_{ji} \in \mathfrak{m}$ for any $i \in I$. Then $\lambda_i = \overline{a_i} = 0$ for any $i \in I$. So $(\overline{e_i})_{i\in I}$ is a k-basis of $F/\mathfrak{m}F$. By definition of f, the induced map $\overline{f} : F/\mathfrak{m}F \to P/\mathfrak{m}P$, $\overline{x} \mapsto \overline{f(x)}$ sends the k-basis $(\overline{e_i})_{i\in I}$ to $(\overline{w_i})_{i\in I}$, which is a k-basis of $P/\mathfrak{m}P$. Then $\overline{f}$ is an isomorphism of k-vector spaces. In particular, it is surjective, i.e. $\operatorname{Coker}(\overline{f}) = (P/\mathfrak{m}P)/\operatorname{Im}(\overline{f}) = 0$. We have that

$$\begin{aligned}\operatorname{Im}\left(\overline{f}\right) = \left\{\overline{y} \in P/\mathfrak{m}P \;\middle|\; \exists \overline{x} \in F/\mathfrak{m}F \quad \overline{y} = \overline{f}(\overline{x}) = \overline{f(x)}\right\} = \\ = \left\{\overline{f(x)} \;\middle|\; x \in F\right\} = (\operatorname{Im}(f) + \mathfrak{m}F)/\mathfrak{m}F \ .\end{aligned}$$

So

$$\begin{aligned}0 = \operatorname{Coker}(\overline{f}) = (P/\mathfrak{m}P)/((\operatorname{Im}(f) + \mathfrak{m}F)/\mathfrak{m}F) \cong \\ \cong (P/\operatorname{Im}(f))/\mathfrak{m}(P/\operatorname{Im}(f)) = \operatorname{Coker}(f)/\mathfrak{m}\operatorname{Coker}(f) \ .\end{aligned}$$

This means that $\mathfrak{m}\operatorname{Coker}(f) = \operatorname{Coker}(f)$. Moreover, we have that $\operatorname{Coker}(f)$ is finitely generated over A ($(w_1{+}\operatorname{Im}(f),\dots,w_n{+}\operatorname{Im}(f))$ is a set of generators). By Nakayama's lemma, this implies that $\operatorname{Coker}(f) = 0$, i.e. f is surjective. Then the sequence

$$0 \to \operatorname{Ker}(f) \to F \xrightarrow{f} P \to 0$$

is exact. By lemma 2.1.14 ((i) $\Longrightarrow$ (iii)), this sequence splits, because P is projective. So there is an isomorphism $\varphi : F \to P \oplus \operatorname{Ker}(f)$. Consider the projection $p_2 : P \oplus \operatorname{Ker}(f) \to \operatorname{Ker}(f)$, which is clearly A-linear and surjective. Then $p_2 \circ \varphi : F \to \operatorname{Ker}(f)$ is an A-linear and projective map. It follows that $((p_2 \circ \varphi)(e_i))_{i\in I}$ generates $\operatorname{Ker}(f)$. In particular, $\operatorname{Ker}(f)$ is finitely generated. Moroever, since $F \cong P \oplus \operatorname{Ker}(f)$, we have that $F/\mathfrak{m}F \cong (P \oplus \operatorname{Ker}(f))/\mathfrak{m}(P \oplus \operatorname{Ker}(f))$. But $\mathfrak{m}(P \oplus \operatorname{Ker}(f)) = (\mathfrak{m}P) \oplus (\mathfrak{m}\operatorname{Ker}(f))$. Indeed, if $(x,y) \in \mathfrak{m}(P \oplus \operatorname{Ker}(f))$, then there exist $a_1,\dots,a_m \in \mathfrak{m}$, $(x_1,y_1),\dots,(x_n,y_n) \in P \oplus \operatorname{Ker}(f)$ ($m \in \mathbb{N}$) such that $(x,y) = \sum_{j=1}^m a_j(x_j,y_j) = \left(\sum_{j=1}^m a_j x_j, \sum_{j=1}^m a_j y_j\right) \in (\mathfrak{m}P) \oplus (\mathfrak{m}\operatorname{Ker}(f))$. Conversely, if $(x,y) \in (\mathfrak{m}P) \oplus (\mathfrak{m}\operatorname{Ker}(f))$, then there exist $a_1,\dots,a_m \in \mathfrak{m}$, $x_1,\dots,x_m \in P$ ($m \in \mathbb{N}$) such that $x = \sum_{j=1}^m a_j x_j$ and $b_1,\dots,b_r \in \mathfrak{m}$, $y_1,\dots,y_r \in \operatorname{Ker}(f)$ ($r \in \mathbb{N}$) such that $y = \sum_{j=1}^r b_j y_j$. Then

$$\begin{aligned}(x,y) = (x,0) + (y,0) = \left(\sum_{j=1}^m a_j x_j, 0\right) + \left(0, \sum_{j=1}^r b_j y_j\right) = \\ = \sum_{j=1}^m a_j (x_j,0) + \sum_{j=1}^r b_j (0,y_j) \in \mathfrak{m}(P \oplus \operatorname{Ker}(f)) \ .\end{aligned}$$

So

$$F/\mathfrak{m}F \cong (P \oplus \operatorname{Ker}(f))/((\mathfrak{m}P) \oplus (\mathfrak{m}\operatorname{Ker}(f))) \cong (P/\mathfrak{m}P) \oplus (\operatorname{Ker}(f)/\mathfrak{m}\operatorname{Ker}(f)),$$

as A-modules and so also k-vector spaces. Then we have

$$|I| = \dim_k(F/\mathfrak{m}F) = \dim_k(P/\mathfrak{m}P) + \dim_k(\operatorname{Ker}(f)/\mathfrak{m}\operatorname{Ker}(f)) = \\ = |I| + \dim_k(\operatorname{Ker}(f)/\mathfrak{m}\operatorname{Ker}(f))$$

(recall that $(\overline{w_i})_{i\in I}$ is a k-basis of $P/\mathfrak{m}P$ and $(\overline{e_i})_{i\in I}$ is a k-basis of $F/\mathfrak{m}F$). It follows that $\dim_k(\operatorname{Ker}(f)/\mathfrak{m}\operatorname{Ker}(f)) = 0$, i.e. $\operatorname{Ker}(f)/\mathfrak{m}\operatorname{Ker}(f) = 0$. This means that $\mathfrak{m}\operatorname{Ker}(f) = \operatorname{Ker}(f)$. Since $\operatorname{Ker}(f)$ is finitely generated, by Nakayama's lemma this implies that $\operatorname{Ker}(f) = 0$. So f is injective. Hence f is an isomorphism of A-modules and $P \cong F$ is free. □

Lemma 2.1.24. *Let P be an A-module and B an A-algebra. If P is a projective A-module, then $P \otimes_A B$ is a projective B-module.*

Proof. Since P is projective, by lemma 2.1.14 ((i) $\Longrightarrow$ (iv)) there exists an A-module Q such that $P\oplus Q$ is free, i.e. we have an isomorphism of A-modules $P\oplus Q \cong \bigoplus_{i\in I} A$, for some index set I. By lemma 2.1.19, we have that

$$(P\otimes_A B)\oplus(Q\otimes_A B) \cong (P\oplus Q)\otimes_A B \cong \left(\bigoplus_{i\in I} A\right)\otimes_A B \cong \bigoplus_{i\in I}(A\otimes_A B) \cong \bigoplus_{i\in I} B$$

(the last isomorphism comes from the canonical isomorphism of B-modules $A\otimes_A B \to B$, $a\otimes b \mapsto ab$). Notice that lemma 2.1.19 gives only an isomorphism of A-modules. However, it is immediate to check that in this case (i.e. when we consider the tensor product with an A-algebra B) the isomorphism we defined is also B-linear. So $(P\otimes_A B)\oplus(Q\otimes_A B) \cong \bigoplus_{i\in I} B$ is a free B-module. By lemma 2.1.14 ((iv) $\Longrightarrow$ (i)), we have that $P\otimes_A B$ is a projective B-module. □

Recall the definition of finitely presented A-module.

Definition 2.1.25. Let M be an A-module. We say that M is *finitely presented* if there exists an exact sequence $A^m \to A^n \to M \to 0$, with $m, n \in \mathbb{N}$.

Remark 2.1.26. An A-module M is finitely presented if and only if there exist $n \in \mathbb{N}$ and a surjective A-linear map $f : A^n \to M$ such that $\operatorname{Ker}(f)$ is finitely generated. Indeed, if $A^m \xrightarrow{\iota} A^n \xrightarrow{f} M \to 0$ is an exact sequence as in the definition, then $\operatorname{Ker}(f) = \operatorname{Im}(i)$ is generated by $(\iota(e_1), \dots, \iota(e_m))$, where $(e_1, \dots, e_m)$ is a basis of A^m (for example, the canonic one). Conversely, if $f : A^n \to M$ is surjective and $\operatorname{Ker}(f)$ is finitely generated, then choose a set of generators $(w_1, \dots, w_m)$ of $\operatorname{Ker}(f)$ ($m \in \mathbb{N}$) and consider the A-linear map $\iota : A^m \to A^n$ with $\iota(e_i) = w_i$ for any $i = 1, \dots, m$ (extended by linearity). Then $\operatorname{Im}(\iota) = \operatorname{Ker}(f)$ and so the sequence $A^m \xrightarrow{\iota} A^n \xrightarrow{f} M \to 0$ is exact.

Lemma 2.1.27. *Let M, N be A-modules, with M finitely presented, and let $S \subseteq A$ be a multiplicative subset. The map*

$$\varphi : S^{-1}\operatorname{Hom}_A(M,N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N),\ \frac{f}{s} \mapsto \frac{1}{s}S^{-1}f\ .$$

is an isomorphism of $S^{-1}A$-modules.

Proof. Since M is finitely presented, there exists an exact sequence $A^m \xrightarrow{\alpha} A^n \xrightarrow{\beta} M \to 0$, with $m, n \in \mathbb{N}$. Define $w_i := \beta(e_i) \in M$ for any $i = 1, \dots, n$, where $(e_1, \dots, e_n)$ is the canonical basis of A^n. Then $(w_1, \dots, w_n)$ generates M, because β is surjective. Moreover, define $x_i := \alpha(e'_i) \in A^n$ for any $i = 1, \dots, m$, where $(e'_1, \dots, e'_m)$ is the canonical basis of A^m. Then $(x_1, \dots, x_n)$ generates $\operatorname{Im}(\alpha) = \operatorname{Ker}(\beta)$.
First of all, we have to check that φ is well defined. We know that for any $f \in \operatorname{Hom}_A(M,N)$ the map $S^{-1}f : S^{-1}M \to S^{-1}N$ is $S^{-1}(A)$-linear. So for any $s \in S$ we have that $\frac{1}{s}S^{-1}f \in \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$. Assume now that $\frac{f}{s} = \frac{f'}{s'}$, with $f, f' \in \operatorname{Hom}_A(M,N)$, $s, s' \in S$. Then there exists $u \in S$ such that $u(s'f - sf') = 0$. Let $\frac{m}{t} \in S^{-1}M$, with $m \in M$ and $t \in S$. Then

$$\left(\frac{1}{s}S^{-1}f\right)\left(\frac{m}{t}\right) = \frac{1}{s}\left((S^{-1}f)\left(\frac{m}{t}\right)\right) = \frac{1}{s}\frac{f(m)}{t} = \frac{f(m)}{st}$$

and analogously $\left(\frac{1}{s'}S^{-1}f'\right)\left(\frac{m}{t}\right) = \frac{f'(m)}{s't}$. We have that

$$u((s't)f(m) - (st)f'(m)) = tu(s'f(m) - sf(m)) = t(u(s'f - sf'))(m) = 0\ .$$

So $\frac{f(m)}{st} = \frac{f'(m)}{s't}$ and then $\frac{1}{s}S^{-1}f = \frac{1}{s'}S^{-1}f'$. This proves that φ is well defined. We prove now that it is $S^{-1}A$-linear. Notice that

$$S^{-1} : \operatorname{Hom}_A(M,N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$$

is A-linear. Let $\lambda_1 = \frac{a_1}{s_1}, \lambda_2 = \frac{a_2}{s_2} \in S^{-1}A$, $\frac{f_1}{t_1}, \frac{f_2}{t_2} \in S^{-1}\operatorname{Hom}_A(M,N)$ (with $a_1, a_2 \in A$, $s_1, s_2, t_1, t_2 \in S$ and $f_1, f_2 \in \operatorname{Hom}_A(M,N)$). We have that

$$\begin{aligned}
\varphi\left(\lambda_1\frac{f_1}{t_1} + \lambda_2\frac{f_2}{t_2}\right) &= \varphi\left(\frac{s_2t_2a_1f_1 + s_1t_1a_2f_2}{s_1s_2t_1t_2}\right) = \\
&= \frac{1}{s_1s_2t_1t_2}S^{-1}(s_2t_2a_1f_1 + s_1t_1a_2f_2) = \frac{1}{s_1s_2t_1t_2}\left(s_2t_2a_1S^{-1}f_1 + s_1t_1a_2S^{-1}f_2\right) = \\
&= \frac{a_1}{s_1}\frac{1}{t_1}S^{-1}f_1 + \frac{a_2}{s_2}\frac{1}{t_2}S^{-1}f_2 = \lambda_1\varphi(f_1) + \lambda_2\varphi(f_2)\ .
\end{aligned}$$

So φ is $S^{-1}A$-linear. Let $\frac{f}{s} \in \operatorname{Ker}(\varphi)$, i.e. $\varphi\left(\frac{f}{s}\right) = 0$. For any $i = 1, \dots, n$, we have that

$$0 = \varphi\left(\frac{f}{s}\right)\left(\frac{w_i}{1}\right) = \left(\frac{1}{s}S^{-1}f\right)\left(\frac{w_i}{1}\right) = \frac{f(w_i)}{s}$$

(see the computation above). Then there exists $u_i \in S$ such that $u_if(w_i) = u_i(1 \cdot f(m) - 0 \cdot s) = 0$. Let $u := u_1 \cdots u_n \in S$. Then for any $i \in I$ we have that

$uf(w_i) = \left(\prod_{j\neq i} u_j\right) u_i f(w_i) = 0$. Then $uf = 0$, because $(w_1, \dots, w_n)$ generates m. We have that $\frac{f}{s} = \frac{uf}{us} = \frac{0}{us} = 0$. This proves that φ is injective.
Let now $g \in \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$. For any $i = 1, \dots, n$ we have that $g\left(\frac{w_i}{1}\right) \in S^{-1}N$ and so there exist $n_i \in N$ and $s_i \in S$ such that $g\left(\frac{w_i}{1}\right) = \frac{n_i}{s_i}$. Define $s := \prod_{i=1}^n s_i \in S$. Then for any $i = 1, \dots, n$ we have that $g\left(\frac{w_i}{1}\right) = \frac{n_i}{s_i} = \frac{(\prod_{j\neq i} s_j)n_i}{(\prod_{j\neq i} s_j)s_i} = \frac{\widetilde{n_i}}{s}$, where we defined $\widetilde{n_i} := \left(\prod_{j\neq i} s_j\right) n_i \in N$. Consider the A-linear map $f : A^n \to N$ obtained extending by linearity $f(e_i) = \widetilde{n_i}$ for any $i = 1, \dots, n$. Let $j \in \{1, \dots, m\}$. Since $x_j \in A^n$, there exist $a_{j1}, \dots, a_{j_n} \in A$ such that $x_j = \sum_{i=1}^n a_{ji} e_i$. We have that

$$0 = \beta(x_j) = \beta\left(\sum_{i=1}^n a_{ji} e_i\right) = \sum_{i=1}^n a_{ji}\beta(e_i) = \sum_{i=1}^n a_{ji} w_i \ .$$

Then

$$0 = g(0) = g\left(\frac{\sum_{i=1}^n a_{ji} w_i}{1}\right) = \sum_{i=1}^n a_{ji} g\left(\frac{w_i}{1}\right) = \sum_{i=1}^n a_{ji}\frac{\widetilde{n_i}}{s} = \frac{\sum_{i=1}^n a_{ji}\widetilde{n_i}}{s} \ .$$

This means that there exists $u_j \in S$ such that $u_j \left(\sum_{i=1}^n a_{ji}\widetilde{n_i}\right) = 0$. Consider $u := \prod_{j=1}^m u_j$. Then, for any $j = 1, \dots, m$ we have that

$$\begin{aligned} uf(x_j) = uf\left(\sum_{i=1}^n a_{ji} e_i\right) = u\left(\sum_{i=1}^n a_{ji} f(e_i)\right) = \\ = u\left(\sum_{i=1}^n a_{ji}\widetilde{n_i}\right) = \left(\prod_{j'\neq j} u_{j'}\right) u_j \left(\sum_{i=1}^n a_{ji}\widetilde{n_i}\right) = 0 \ . \end{aligned}$$

Define $f' := uf \in \operatorname{Hom}_A(A^n, N)$. By what we have just proved, $f'(x_j) = 0$ for any $j = 1, \dots, m$. Since $(x_1, \dots, x_m)$ generates $\operatorname{Ker}(\beta)$, we have that $f'(x) = 0$ for any $x \in \operatorname{Ker}(\beta)$, i.e. $\operatorname{Ker}(\beta) \subseteq \operatorname{Ker}(f')$. Then we can factor f' through an A-linear map $\overline{f'} : A^n/\operatorname{Ker}(\beta) \to N$ such that $f = \overline{f'} \circ p$, where $p : A^n \to A^n/\operatorname{Ker}(\beta)$ is the canonical projection on the quotient. In particular, $\overline{f'}(e_i + \operatorname{Ker}(\beta)) = f'(e_i) = uf(e_i) = u\widetilde{n_i}$ for any $i = 1, \dots, n$. Since β is surjective, by the isomorphism theorem we have an isomorphism $\overline{\beta} : A^n/\operatorname{Ker}(\beta) \to M$, with $\overline{\beta}(x + \operatorname{Ker}(\beta)) = \beta(x)$ for any $x \in A^n$. In particular, $\overline{\beta}(e_i + \operatorname{Ker}(\beta)) = \beta(e_i) = w_i$ for any $i = 1, \dots, n$. We define $h := \overline{f'} \circ \overline{\beta}^{-1} \in \operatorname{Hom}_A(M, N)$. For any $i = 1, \dots, n$, we have that

$$h(w_i) = \overline{f'}\left(\overline{\beta}^{-1}(w_i)\right) = \overline{f'}(e_i + \operatorname{Ker}(\beta)) = u\widetilde{n_i} \ .$$

Consider $\frac{h}{us} \in S^{-1}\operatorname{Hom}_A(M, N)$. For any $i = 1, \dots, n$ we have

$$\varphi\left(\frac{h}{us}\right)\left(\frac{w_i}{1}\right) = \left(\frac{1}{us}S^{-1}h\right)\left(\frac{w_i}{1}\right) = \frac{h(w_i)}{us} = \frac{u\widetilde{n_i}}{us} = \frac{\widetilde{n_i}}{s} = g\left(\frac{w_i}{1}\right) \ .$$

Since $(w_1, \dots, w_n)$ generates M over A, $(\frac{w_1}{1}, \dots, \frac{w_n}{1})$ generates $S^{-1}M$ over $S^{-1}A$. Then we must have $\varphi\left(\frac{h}{us}\right) = g$. This proves that φ is surjective. □

Lemma 2.1.28. *(1) Let M be an A-module. We have that $M = 0$ if and only if $M_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p}$ of A.*

(2) Let M, N be A-modules and $f : M \to N$ an A-linear map. Then f is surjective (respectively, injective or bijective) if and only if $f_{\mathfrak{p}}$ is surjective (respectively, injective or bijective) for every prime ideal $\mathfrak{p}$ of A.

Proof. (1) It is clear that if $M = 0$ then $M_{\mathfrak{p}} = 0$ for any prime ideal $\mathfrak{p}$. Conversely, assume that $M_{\mathfrak{p}} = 0$ for any prime ideal $\mathfrak{p}$. Assume by contradiction that $M \neq 0$ and let $m \in M \backslash \{0\}$. Then the annihilator $\operatorname{Ann}_A(m)$ is a proper ideal of A, because $1 \notin \operatorname{Ann}_A(m)$. So there exists a maximal ideal $\mathfrak{m}$ such that $\operatorname{Ann}_A(m) \subseteq \mathfrak{m}$. In particular, $\mathfrak{m}$ is prime, so we have that $M_{\mathfrak{m}} = 0$ by assumption. So $\frac{m}{1} = 0$ in $M_{\mathfrak{m}}$. This means that there exists $s \in A \backslash \mathfrak{p}$ such that $sm = 0$. Then $s \in \operatorname{Ann}_A(M) \subseteq \mathfrak{m}$, which is a contradtion. So we must have $M = 0$.

(2) Let $\mathfrak{p}$ be a prime ideal of A. We have that $\operatorname{Coker}(f)_{\mathfrak{p}} = (N/\operatorname{Im}(f))_{\mathfrak{p}} \cong N_{\mathfrak{p}}/\operatorname{Im}(f)_{\mathfrak{p}}$, because the localization commutes with quotients. We have that $\operatorname{Im}(f)_{\mathfrak{p}}$ and $\operatorname{Im}(f_{\mathfrak{p}})$ are submodules of $N_{\mathfrak{p}}$ and

$$\operatorname{Im}(f)_{\mathfrak{p}} = \left\{ \frac{y}{s} \;\middle|\; y \in \operatorname{Im}(f), s \in A \backslash \mathfrak{p} \right\} = \left\{ \frac{f(x)}{s} \;\middle|\; x \in M, s \in A \backslash \mathfrak{p} \right\} =$$
$$= \left\{ f_{\mathfrak{p}}\left(\frac{x}{s}\right) \;\middle|\; \frac{x}{s} \in M_{\mathfrak{p}} \right\} = \operatorname{Im}(f_{\mathfrak{p}}) .$$

So $\operatorname{Coker}(f)_{\mathfrak{p}} \cong N_{\mathfrak{p}}/\operatorname{Im}(f)_{\mathfrak{p}} = N_{\mathfrak{p}}/\operatorname{Im}(f_{\mathfrak{p}}) = \operatorname{Coker}(f_{\mathfrak{p}})$.
On the other hand, consider $\operatorname{Ker}(f) \subseteq M$. For any $x \in \operatorname{Ker}(f)$ and $s \in A \backslash \mathfrak{p}$, we have that $f_{\mathfrak{p}}\left(\frac{x}{s}\right) = \frac{f(x)}{s} = 0$. So $\frac{x}{s} \in \operatorname{Ker}(f_{\mathfrak{p}})$. This shows that $\operatorname{Ker}(f)_{\mathfrak{p}} \subseteq \operatorname{Ker}(f_{\mathfrak{p}})$. Conversely, if $\frac{x}{s} \in \operatorname{Ker}(f_{\mathfrak{p}})$, with $x \in M$ and $s \in A \backslash \mathfrak{p}$, then $0 = f_{\mathfrak{p}}\left(\frac{x}{s}\right) = \frac{f(x)}{s}$. Then there exists $u \in A \backslash \mathfrak{p}$ such that $uf(x) = 0$. Since f is A-linear, we have that $f(ux) = uf(x) = 0$. So $ux \in \operatorname{Ker}(f)$. Then $\frac{x}{s} = \frac{ux}{us} \in \operatorname{Ker}(f)_{\mathfrak{p}}$. So $\operatorname{Ker}(f)_{\mathfrak{p}} = \operatorname{Ker}(f_{\mathfrak{p}})$.
Now we have that f is surjective if and only if $\operatorname{Coker}(f) = 0$ and by point (1) we have that this is true if and only if $\operatorname{Coker}(f_{\mathfrak{p}}) \cong \operatorname{Coker}(f)_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p}$ of A, so if and only if $f_{\mathfrak{p}}$ is surjective for every prime ideal $\mathfrak{p}$ of A.
Analogously, f is injective if and only if $\operatorname{Ker}(f) = 0$ and by point (1) we have that this is true if and only if $\operatorname{Ker}(f_{\mathfrak{p}}) = \operatorname{Ker}(f)_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p}$ of A, so if and only if $f_{\mathfrak{p}}$ is injective for every prime ideal $\mathfrak{p}$ of A. Then we have also that f is bijective if and only if $f_{\mathfrak{p}}$ is bijective for every prime ideal $\mathfrak{p}$ of A. □

For any $f \in A$, we define $S_f := \{f^n \mid n \geq 0\}$, $A_f := S_f^{-1}A$ and $M_f := S_f^{-1}M \cong M \otimes_A A_f$ for any A-module M (then M_f is an A_f-module).

Lemma 2.1.29. *Let $(f_i)_{i \in I}$ be a collection of elements of A such that $A = \sum_{i \in I} f_i A$.*

(1) For every A-module M, we have that $M = 0$ if and only if $M_{f_i} = 0$ for every $i \in I$.

(2) Let M, N be A-modules and $g : M \to N$ an A-linear map. Then g is surjective (respectively, injective or bijective) if and only if $g_{f_i} : M_{f_i} \to N_{f_i}$ is surjective (respectively, injective or bijective) for every $i \in I$.

(3) Let M be an A-module. If M_{f_i} is a finitely generated A_{f_i}-module for every $i \in I$, then M is finitely generated.

Proof. (1) It is clear that if $M = 0$ then $M_{f_i} = 0$ for any $i \in I$. Conversely, assume that $M_{f_i} = 0$ for any $i \in I$. Let $\mathfrak{p}$ be a prime ideal of A. In particular, $\mathfrak{p} \neq A$ and so there exists $i \in I$ such that $f_i \notin \mathfrak{p}$ (otherwise we would have $A = \sum_{i \in I} f_i A \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, it follows that $f_i^n \notin \mathfrak{p}$ for any $n \in \mathbb{N}$, i.e. $S_{f_i} \subseteq A \backslash \mathfrak{p}$. Then we have that $M_{\mathfrak{p}} \cong (M_{f_i})_{\mathfrak{p}_{f_i}} = 0_{\mathfrak{p}_{f_i}} = 0$. Since this holds for every prime ideal $\mathfrak{p}$ of A, by lemma 2.1.28(1) it follows that $M = 0$.

(2) The proof is analogous to that of lemma 2.1.28(2).

(3) Since $\sum_{i \in I} f_i A = A$, we have that $1 \in \sum_{i \in I} f_i A$, i.e. there exist $n \in \mathbb{N}$, $i_1, \ldots, i_n \in I$, $a_1, \ldots, a_n \in A$ such that $1 = \sum_{k=1}^{n} a_k f_{i_k}$. Then for any $x \in A$ we have that $x = x \cdot 1 = x\left(\sum_{k=1}^{n} a_k f_{i_k}\right) = \sum_{k=1}^{n} (x a_k) f_{i_k}$. So $A = \sum_{k=1}^{n} f_{i_k} A$. Let $k \in \{1, \ldots, n\}$ and let $(x_{k1}, \ldots, x_{kr_k})$ be a set of generators of $M_{f_{i_k}}$ over $A_{f_{i_k}}$. By definition of localization, for any $h = 1, \ldots, r_k$ there exist $m_{kh} \in M$, $n_{kh} \in \mathbb{N}$ such that $x_{kh} = \frac{m_{kh}}{f_{i_k}^{n_{kh}}}$. For any $x \in M_{f_{i_k}}$, there exist $\lambda_1, \ldots, \lambda_{r_k} \in M_{f_{i_k}}$ such that

$$x = \sum_{h=1}^{r_k} \lambda_h x_{kh} = \sum_{h=1}^{r_k} \lambda_h \frac{m_{kh}}{f_{i_k}^{n_{kh}}} = \sum_{h=1}^{r_k} \left(\lambda_h \frac{1}{f_{i_k}^{n_{kh}}} \right) \frac{y_{mh}}{1} .$$

This proves that $\left(\frac{m_{k1}}{1}, \ldots, \frac{m_{kr_k}}{1}\right)$ is a set of generators of $M_{f_{i_k}}$ over $A_{f_{i_k}}$. We claim that $(m_{kh})_{k=1,\ldots,n,\, h=1,\ldots,r_k}$ generates M. Let $N \subseteq M$ be the submodule generated by $(m_{kh})_{k=1,\ldots,n,\, h=1,\ldots,r_k}$ and consider the quotient M/N. Let $k \in \{1, \ldots, n\}$. We have that $(M/N)_{f_{i_k}} \cong M_{f_{i_k}}/N_{f_{i_k}}$, because the localization commutes with quotients. On the other hand, we have that $N_{f_{i_k}}$ contains $\frac{m_{kh}}{1}$ for any $h = 1, \ldots, r_k$. Since $\left(\frac{m_{k1}}{1}, \ldots, \frac{m_{kr_k}}{1}\right)$ generates $M_{f_{i_k}}$ over $A_{f_{i_k}}$, we have that $N_{f_{i_k}} = M_{f_{i_k}}$. So $M_{f_{i_k}}/N_{f_{i_k}} = 0$. Then $(M/N)_{f_{i_k}} = 0$ and this holds for any $k = 1, \ldots, n$. Applying point (1) to the collection $(f_{i_k})_{k=1,\ldots,n}$, we get that $M/N = 0$, i.e. $M = N$. This proves that M is generated by $(m_{kh})_{k=1,\ldots,n,\, h=1,\ldots,r_k}$. Since this is a finite set, M is finitely generated.

□

We are now ready to give our local characterization.

Proposition 2.1.30. *Let P be an A-module. The following are equivalent:*

(i) P is a finitely generated projective A-module;

(ii) P is finitely presented and for any prime ideal $\mathfrak{p}$ of A we have that $P_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module;

(iii) P is finitely presented and for any maximal ideal $\mathfrak{m}$ of A we have that $P_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module;

(iv) there is a collection $(f_i)_{i\in I}$ of elements of A such that $\sum_{i\in I} f_iA = A$ and for each $i \in I$ the A_{f_i}-module P_{f_i} is free of finite rank.

Proof. (i) $\Longrightarrow$ (ii) Since P is finitely generated and projective, by corollary 2.1.15 there exist an A-module Q and an $n \in \mathbb{N}$ such that $A^n \cong P \oplus Q$. Let $\varphi : A^n \to P \oplus Q$ be an isomorphism. Denote by $p_1 : P \oplus Q \to P$ and $p_2 : P \oplus Q \to Q$ the canonical projections, which are A-linear and surjective. We have that $p_1 \circ \varphi : A^n \to P$ is surjective, because φ is an isomorphism and p_1 is surjective. Moreover, $\mathrm{Ker}(p_1 \circ \varphi) = \varphi^{-1}(\mathrm{Ker}(p_1)) = \varphi^{-1}(\mathrm{Im}(\iota_2))$, where we defined $\iota_2 : Q \to P \oplus Q,\ x \mapsto (0, x)$. We have that $p_2 \circ \varphi$ is surjective, because φ is an isomorphism and p_2 is surjective. Then Q is generated by $((p_2\circ\varphi)(e_1), \ldots, (p_2\circ\varphi)(e_n))$ and $\mathrm{Im}(\iota_2)$ is generated by $((\iota_2\circ p_2\circ\varphi)(e_1), \ldots, (\iota_2\circ p_2\circ\varphi)(e_n))$, where $(e_1, \ldots, e_n)$ is the canonical basis of A^n. So $\mathrm{Im}(\iota_2)$ is finitely generated. Since φ is an isomorphism, we have also that $\mathrm{Ker}(p_1 \circ \varphi) = \varphi^{-1}(\mathrm{Im}(\iota_2))$ is finitely generated. This proves that P is finitely presented (see remark 2.1.26).
Let $\mathfrak{p}$ be a prime ideal of A. Since localization at $\mathfrak{p}$ corresponds to tensor product with $A_\mathfrak{p}$, by lemma 2.1.24 we have that $P_\mathfrak{p}$ is projective over $A_\mathfrak{p}$. Moreover, if $(w_1, \ldots, w_m)$ generates P over A, then we have that $(\frac{w_1}{1}, \ldots, \frac{w_m}{1})$ generates $P_\mathfrak{p}$ over $A_\mathfrak{p}$. So $P_\mathfrak{p}$ is finitely generated over $A_\mathfrak{p}$. Then, by lemma 2.1.23, we have that $P_\mathfrak{p}$ is free over $A_\mathfrak{p}$ (because $A_\mathfrak{p}$ is a local ring).

(ii) $\Longrightarrow$ (iii) This is obvious, because every maximal ideal is prime.

(iii) $\Longrightarrow$ (iv) Let $\mathfrak{m}$ be a maximal ideal of A. By assumption, $P_\mathfrak{m}$ is free over $A_\mathfrak{m}$. Moreover, since P is finitely presented, it is in particular finitely generated over A and so $P_\mathfrak{m}$ is finitely generated over $A_\mathfrak{m}$ (if $(w_1, \ldots, w_n)$ generates P over A, then $\left(\frac{w_1}{1}, \ldots, \frac{w_n}{1}\right)$ generates $P_\mathfrak{m}$ over $A_\mathfrak{m}$). This means that the rank of $P_\mathfrak{m}$ over $A_\mathfrak{m}$ is finite (see remark 2.1.2(1)). So there exists an isomorphism of $A_\mathfrak{m}$-modules $g : A_\mathfrak{m}^{n_\mathfrak{m}} \to P_\mathfrak{m}$, where $n_\mathfrak{m} = \mathrm{rank}_{A_\mathfrak{m}}(P_\mathfrak{m})$. Let $h := g^{-1} : P_\mathfrak{m} \to A_\mathfrak{m}^{n_\mathfrak{m}}$. Notice that $A_\mathfrak{m}^{n_\mathfrak{m}} \cong (A^{n_\mathfrak{m}})_\mathfrak{m}$ as $A_\mathfrak{m}$-modules, because the localization commutes with direct sums. Let $\varphi : A_\mathfrak{m}^{n_\mathfrak{m}} \to (A^\mathfrak{n})_\mathfrak{m}$ be an isomorphism of $A_\mathfrak{m}$-modules. Then $g \circ \varphi^{-1} \in \mathrm{Hom}_{A_\mathfrak{m}}((A^{n_\mathfrak{m}})_\mathfrak{m}, P_\mathfrak{m})$ and $\varphi \circ h \in \mathrm{Hom}_{A_\mathfrak{m}}(P_\mathfrak{m}, (A^{n_\mathfrak{m}})_\mathfrak{m})$. By lemma 2.1.27, there exist $g' \in \mathrm{Hom}_A(A^{n_\mathfrak{m}}, P)$, $h' \in \mathrm{Hom}_A(P, A^{n_\mathfrak{m}})$, $s, t \in A\backslash\mathfrak{m}$ such that $g \circ \varphi^{-1} = \frac{1}{s}(g')_\mathfrak{m}$ and $\varphi \circ h = \frac{1}{t}(h')_\mathfrak{m}$ (here we use the assumption that P is finitely presented; on the other hand it is clear that $A^{n_\mathfrak{m}}$ is finitely presented, because we have the exact sequence $0 \to A^{n_\mathfrak{m}} \xrightarrow{\mathrm{id}_{A^{n_\mathfrak{m}}}} A^{n_\mathfrak{m}} \to 0$). We have that

$$\frac{1}{st}(g'\circ h')_\mathfrak{m} = \left(\frac{1}{s}(g')_\mathfrak{m}\right)\circ\left(\frac{1}{t}(h')_\mathfrak{m}\right) = g\circ\varphi^{-1}\circ\varphi\circ h = g\circ g^{-1} = \mathrm{id}_{P_\mathfrak{m}} = (\mathrm{id}_P)_\mathfrak{m}\ .$$

By injectivity in lemma 2.1.27, this implies that $\frac{g'\circ h'}{st} = \mathrm{id}_P$ in $\mathrm{Hom}_A(P, P)_\mathfrak{m}$ (we use again the fact that P is finitely presented). This means that there exists $u \in A\backslash\mathfrak{m}$ such that $u(g' \circ h' - st\,\mathrm{id}_P) = 0$. On the other hand, we have that

$$\frac{1}{st}(h'\circ g')_{\mathfrak{m}} = \left(\frac{1}{t}(h')_{\mathfrak{m}}\right)\circ\left(\frac{1}{s}(g')_{\mathfrak{m}}\right) = \\ = \varphi\circ h\circ g\circ\varphi^{-1} = \varphi\circ g^{-1}\circ g\circ\varphi^{-1} = \mathrm{id}_{(A^{n_{\mathfrak{m}}})_{\mathfrak{m}}} = (\mathrm{id}_{A^{n_{\mathfrak{m}}}})_{\mathfrak{m}} \ .$$

By injectivity in lemma 2.1.27, this implies $\frac{h'\circ g'}{st} = \mathrm{id}_{A^{n_{\mathfrak{m}}}}$ in $\mathrm{Hom}_A(A^{n_{\mathfrak{m}}}, A^{n_{\mathfrak{m}}})_{\mathfrak{m}}$ (we use again the fact that $A^{n_{\mathfrak{m}}}$ is finitely presented). This means that there exists $v \in A\backslash\mathfrak{m}$ such that $v(h'\circ g' - st\,\mathrm{id}_{A^{n_{\mathfrak{m}}}}) = 0$. Define $f_{\mathfrak{m}} := stuv$ (everything we defined up to now depended on $\mathfrak{m}$, but we did not make explicit this dependence in the notation in order to avoid confusion). Since $A\backslash\mathfrak{m}$ is a multiplicative subset of A, we have that $f_{\mathfrak{m}} \in A\backslash\mathfrak{m}$. Define $g'' := \frac{tuvg'}{f_{\mathfrak{m}}} \in \mathrm{Hom}_A(A^{n_{\mathfrak{m}}}, P)_{f_{\mathfrak{m}}}$ and $h'' := \frac{suvh'}{f_{\mathfrak{m}}} \in \mathrm{Hom}_A(A^{n_{\mathfrak{m}}}, P)_{f_{\mathfrak{m}}}$. We can associate to g'' and h'' the two maps $\widetilde{g} = \frac{1}{f_{\mathfrak{m}}}(tuvg')_{f_{\mathfrak{m}}} \in \mathrm{Hom}_{A_{f_{\mathfrak{m}}}}((A^{n_{\mathfrak{m}}})_{f_{\mathfrak{m}}}, P_{f_{\mathfrak{m}}})$ and $\widetilde{h} = \frac{1}{f_{\mathfrak{m}}}(suvh')_f \in \mathrm{Hom}_{A_{f_{\mathfrak{m}}}}(P_{f_{\mathfrak{m}}}, (A^{n_{\mathfrak{m}}})_{f_{\mathfrak{m}}})$, as in lemma 2.1.27. We have that

$$\widetilde{g}\circ\widetilde{h} = \left(\frac{1}{f_{\mathfrak{m}}}(tuvg')_{f_{\mathfrak{m}}}\right)\circ\left(\frac{1}{f_{\mathfrak{m}}}(suvh')_{f_{\mathfrak{m}}}\right) = \frac{tuvsv}{f_{\mathfrak{m}}^2}(ug'\circ h')_{f_{\mathfrak{m}}} = \\ = \frac{tuvsv}{f_{\mathfrak{m}}^2}(ust\,\mathrm{id}_P)_{f_{\mathfrak{m}}} = \frac{s^2t^2u^2v^2}{f_{\mathfrak{m}}^2}(\mathrm{id}_P)_{f_{\mathfrak{m}}} = \frac{f_{\mathfrak{m}}^2}{f_{\mathfrak{m}}^2}\mathrm{id}_{P_{f_{\mathfrak{m}}}} = \mathrm{id}_{P_{f_{\mathfrak{m}}}} \ .$$

Conversely,

$$\widetilde{h}\circ\widetilde{g} = \left(\frac{1}{f_{\mathfrak{m}}}(suvh')_{f_{\mathfrak{m}}}\right)\circ\left(\frac{1}{f_{\mathfrak{m}}}(tuvg')_{f_{\mathfrak{m}}}\right) = \frac{suvtu}{f_{\mathfrak{m}}^2}(vh'\circ g')_{f_{\mathfrak{m}}} = \\ = \frac{suvtu}{f_{\mathfrak{m}}^2}(vst\,\mathrm{id}_{A^{n_{\mathfrak{m}}}})_{f_{\mathfrak{m}}} = \frac{s^2t^2u^2v^2}{f_{\mathfrak{m}}^2}(\mathrm{id}_{A^{n_{\mathfrak{m}}}})_{f_{\mathfrak{m}}} = \mathrm{id}_{(A^{n_{\mathfrak{m}}})_{f_{\mathfrak{m}}}} \ .$$

So $\widetilde{g}$ and $\widetilde{h}$ are inverse to each other. In particular, they are isomorphisms of $A_{f_{\mathfrak{m}}}$-modules. Then $P_{f_{\mathfrak{m}}} \cong (A^{n_{\mathfrak{m}}})_{f_{\mathfrak{m}}}$ as $A_{f_{\mathfrak{m}}}$-modules. On the other hand, we have that $(A^{n_{\mathfrak{m}}})_{f_{\mathfrak{m}}} \cong A_{f_{\mathfrak{m}}}^{n_{\mathfrak{m}}}$ as $A_{f_{\mathfrak{m}}}$-modules, because the localization commutes with direct sums. So $P_{f_{\mathfrak{m}}} \cong A_{f_{\mathfrak{m}}}^{n_{\mathfrak{m}}}$ is a free $A_{f_{\mathfrak{m}}}$-module of rank $n_{\mathfrak{m}}$ (in particular, the rank is finite). Let now I be the set of all maximal ideals of A and consider the collection $(f_{\mathfrak{m}})_{\mathfrak{m}\in I}$. For any maximal ideal $\mathfrak{m}_0$ we have that $f_{\mathfrak{m}_0} \in \left(\sum_{\mathfrak{m}\in I} f_{\mathfrak{m}}A\right)\backslash\mathfrak{m}_0$, so $\sum_{\mathfrak{m}\in I} f_{\mathfrak{m}}A \nsubseteq \mathfrak{m}_0$. Then we must have $\sum_{\mathfrak{m}\in I} f_{\mathfrak{m}}A = A$ (recall that any proper ideal is contained in a maximal ideal). So the collection $(f_{\mathfrak{m}})_{\mathfrak{m}\in I}$ satisfies the required properties.

(iv) $\Longrightarrow$ (i) Since $\sum_{i\in I} f_iA = A$, we have that $1 \in \sum_{i\in I} f_iA$, i.e. there exist $n\in\mathbb{N}$, $i_1,\dots,i_n \in I$, $a_1,\dots,a_n \in A$ such that $1 = \sum_{k=1}^n a_kf_{i_k}$. Then for any $x\in A$ we have that $x = x\cdot 1 = x\left(\sum_{k=1}^n a_kf_{i_k}\right) = \sum_{k=1}^n (xa_k)f_{i_k}$. So $A = \sum_{k=1}^n f_{i_k}A$. Then, replacing I with $\{i_1,\dots i_n\}$, we can assume without loss of generality that I is finite.

The fact that P is finitely generated follows from lemma 2.1.29(3). In order to prove that P is projective, we prove firstly that it is finitely presented (this will allow us to apply lemma 2.1.27). Let $i\in I$. By assumption, we have that

P_{f_i} is free of finite rank over A_{f_i}. Let $n(i) := \text{rank}_{A_{f_i}}(P_{f_i})$. Then we have an isomorphism of A_{f_i}-modules $g_i : A_{f_i}^{n(i)} \to P_{f_i}$. Let $(e_{i1}, \ldots, e_{in(i)})$ be the canonical basis of $A_{f_i}^{n(i)}$. For any $k = 1, \ldots, n(i)$, we have that $g_i(e_{ik}) \in P_{f_i}$, so by definition of localization there exist $x_{ik} \in P$, $m_{ik} \in \mathbb{N}$ such that $g_i(e_{ik}) = \frac{x_{ik}}{f_i^{m_{ik}}}$. Let $m_i := \max_{k=1,\ldots,n(i)} m_{ik}$. Then, for any $k = 1, \ldots, n(i)$, we have

$$g_i(e_{ik}) = \frac{x_{ik}}{f_i^{m_{ik}}} = \frac{f_i^{m_i - m_{ik}} x_{ik}}{f_i^{m_i - m_{ik}} f_i^{m_{ik}}} = \frac{\widetilde{x_{ik}}}{f_i^{m_i}} \ ,$$

where we defined $\widetilde{x_{ik}} := f_i^{m_i - m_{ik}} x_{ik} \in P$. Define now $h_i := f_i^{m_i} g_i : A_{f_i}^{n(i)} \to P_{f_i}$. Then h_i is an isomorphism of A_{f_i}-modules, with inverse $\frac{1}{f_i^{m_i}} g^{-1}$. Define moreover an A-linear map $h'_i : A^{n(i)} \to P$ by $h'_i(e'_{ik}) = \widetilde{x_{ik}}$ for any $k = 1, \ldots, n(i)$ (extended by linearity), where $(e'_{i1}, \ldots, e'_{in(i)})$ is the canonical basis of $A^{n(i)}$. Localizing we get an A_{f_i}-linear map $(h'_i)_{f_i} : (A^{n(i)})_{f_i} \to P_{f_i}$. Since the localization commutes with direct sums, we have an isomorphism of A_{f_i}-modules $\varphi_i : (A^{n(i)})_{f_i} \to A_{f_i}^{n(i)}$. This isomorphism sends $\frac{e'_{ik}}{1}$ to e_{ik} for any $k = 1, \ldots, n(i)$. Consider then $h_i \circ \varphi_i \in \text{Hom}_{A_{f_i}}((A^{n(i)})_{f_i}, P_{f_i})$. For any $k = 1, \ldots, n(i)$, we have that

$$(h_i \circ \varphi_i)\left(\frac{e'_{ik}}{1}\right) = h_i(e_{ik}) = f_i^{m_i} g_i(e_{ik}) =$$
$$= f_i^{m_i} \frac{\widetilde{x_{ik}}}{f_i^{m_i}} = \frac{\widetilde{x_{ik}}}{1} = \frac{h'_i(e'_{ik})}{1} = (h'_i)_{f_i}\left(\frac{e'_{ik}}{1}\right) \ .$$

So $h_i \circ \varphi_i = (h'_i)_{f_i}$. Since both h_i and φ_i are isomorphisms, it follows that $(h'_i)_{f_i}$ is an isomorphism of A_{f_i}-modules. Define now $F := \bigoplus_{i \in I} A^{n(i)}$ and

$$h' : F \to P, \ (x_i)_{i \in I} \mapsto \sum_{i \in I} h'_i(x_i) \ .$$

This map is A-linear because it is equal to $\varphi'_P((h'_i)_{i \in I})$, where

$$\varphi'_P : \prod_{i \in I} \text{Hom}_A(A^{n(i)}, P) \to \text{Hom}_A(F, P)$$

is defined as in lemma 2.1.9. Moreover, for any $i \in I$, we have $h' \circ q_i = h'_i$, where we defined $q_i : A^{n(i)} \to F$, $x \mapsto (\delta_{ij} x)_{j \in I}$. We know that $(h')_{f_i} \circ (q_i)_{f_i} = (h' \circ q_i)_{f_i} = (h'_i)_{f_i}$ is an isomorphism, in particular it is surjective. It follows that $(h')_{f_i}$ is surjective. Since this holds for any $i \in I$, by lemma 2.1.29(2) we have that h' is surjective. Moreover, consider $\text{Ker}(h') \subseteq F$. Let $i \in I$. As in the proof of lemma 2.1.28(2), we have that $\text{Ker}(h')_{f_i} = \text{Ker}((h')_{f_i})$. We claim now that $\text{Ker}((h')_{f_i})$ is finitely generated over A_{f_i}. Since $h_i : A_{f_i}^{n(i)} \to P_{f_i}$ is an isomorphism of A_{f_i}-modules, we have that $(h_i(e_{i1}), \ldots, h_i(e_{in(i)})) = \left(\frac{\widetilde{x_{i1}}}{1}, \ldots, \frac{\widetilde{x_{in(i)}}}{1}\right)$ is a basis of P_{f_i} as an A_{f_i}-module. We have also that

$$\frac{\widetilde{x_{ik}}}{1} = (h'_i)_{f_i}\left(\frac{e'_{ik}}{1}\right) = ((h')_{f_i} \circ (q_i)_{f_i})\left(\frac{e'_{ik}}{1}\right) = (h')_{f_i}\left(\frac{q_i(e'_{ik})}{1}\right) \ ,$$

for any $k = 1, \dots, n(i)$. Consider now $j \in I$, $j \neq i$ and the A_{f_i}-linear map $(h' \circ q_j)_{f_i} = (h')_{f_i} \circ (q_j)_{f_i} : (A^{n(j)})_{f_i} \to P_{f_i}$. For any $k = 1, \dots, n(j)$, we have that $(h')_{f_i}\left(\frac{q_j(e'_{jk})}{1}\right) = ((h')_{f_i} \circ (q_j)_{f_i})\left(\frac{e'_{jk}}{1}\right) \in P_{f_i}$, so there exist $\lambda_{jk1}, \dots, \lambda_{jkn(i)} \in A_{f(i)}$ such that

$$(h')_{f_i}\left(\frac{q_j(e'_{jk})}{1}\right) = \sum_{r=1}^{n(i)} \lambda_{jkr}\frac{\widetilde{x_{ir}}}{1} = \sum_{r=1}^{n(i)} \lambda_{jkr}(h')_{f_i}\left(\frac{q_i(e'_{ir})}{1}\right) .$$

Since $(h')_{f_i}$ is A_{f_i}-linear, this implies that

$$(h')_{f_i}\left(\frac{q_j(e'_{jk})}{1} - \sum_{r=1}^{n(i)} \lambda_{jkr}\frac{q_i(e'_{ir})}{1}\right) = 0 ,$$

i.e. $y_{jk} := \frac{q_j(e'_{jk})}{1} - \sum_{r=1}^{n(i)} \lambda_{jkr}\frac{q_i(e'_{ir})}{1} \in \mathrm{Ker}((h')_{f_i})$. Denote now by M the A_{f_i}-submodule of F_{f_i} generated by $(y_{jk})_{j\in I,\, j\neq i,\, k=1,\dots,n(j)}$. Since I is finite, we have that M is finitely generated. Moreover, since $\mathrm{Ker}((h')_{f_i})$ is an A_{f_i}-submodule of F_{f_i}, we have that $M \subseteq \mathrm{Ker}((h')_{f_i})$. Let $x \in \mathrm{Ker}((h')_{f_i})$, i.e. $(h')_{f_i}(x) = 0$. Notice that F is generated by $(q_j(e'_{jk}))_{j\in I,\, k=1,\dots,n(j)}$. Then F_{f_i} is generated by $\left(\frac{q_j(e'_{jk})}{1}\right)_{j\in I,\, k=1,\dots,n(j)}$ over A_{f_i}. So there exist $\mu_{jk} \in A_{f_i}$ (for any $j \in I$, $k = 1, \dots, n(j)$) such that $x = \sum_{j\in J,\, k=1,\dots,n(j)} \mu_{jk}\frac{q_j(e'_{jk})}{1}$. Then we have

$$\begin{aligned} x = \sum_{k=1}^{n(i)} \mu_{ik}\frac{q_i(e'_{ik})}{1} + \sum_{\substack{j\in I\setminus\{i\}\\ k=1,\dots,n(j)}} \mu_{jk}\left(\frac{q_j(e'_{jk})}{1} - \sum_{r=1}^{n(i)} \lambda_{jkr}\frac{q_i(e'_{ir})}{1}\right) + \\ + \sum_{\substack{j\in I\setminus\{i\}\\ k=1,\dots,n(j)}} \mu_{jk}\sum_{r=1}^{n(i)} \lambda_{jkr}\frac{q_i(e'_{ir})}{1} = \\ = \sum_{r=1}^{n(i)} \mu_{ir}\frac{q_i(e'_{ir})}{1} + \sum_{\substack{j\in I\setminus\{i\}\\ k=1,\dots,n(j)}} \mu_{jk}y_{jk} + \sum_{r=1}^{n(i)} \frac{q_i(e'_{ir})}{1}\left(\sum_{\substack{j\in I\setminus\{i\}\\ k=1,\dots,n(j)}} \mu_{jk}\lambda_{jkr}\right) = \\ = \sum_{r=1}^{n(i)} \frac{q_i(e'_{ir})}{1}\left(\mu_{ir} + \sum_{\substack{j\in I\setminus\{i\}\\ k=1,\dots,n(j)}} \mu_{jk}\lambda_{jkr}\right) + y , \end{aligned}$$

where we defined $y := \sum_{\substack{j\in I\setminus\{i\}\\ k=1,\dots,n(j)}} \mu_{jk}y_{jk} \in M$. Define also $\nu_{ir} := \mu_{ir} + \sum_{j\in I\setminus\{i\},\, k=1,\dots,n(j)} \mu_{jk}\lambda_{jkr} \in A_{f_i}$, for any $r = 1, \dots, n(i)$. Then we get that $x = \sum_{r=1}^{n(i)} \nu_{ir}\frac{q_i(e'_{ir})}{1} + y$. Since $M \subseteq \mathrm{Ker}((h')_{f_i})$, we have that $(h')_{f_i}(y) = 0$.

So, applying the A_{f_i}-linearity of $(h')_{f_i}$, we get

$$0 = (h')_{f_i}(x) = \sum_{r=1}^{n(i)} \nu_{ir}(h')_{f_i}\left(\frac{q_i(e'_{ir})}{1}\right) + (h')_{f_i}(y) = \sum_{r=1}^{n(i)} \nu_{ir}\frac{\widetilde{x_{ik}}}{1}\ .$$

But we know that $\left(\frac{\widetilde{x_{i1}}}{1}, \dots, \frac{\widetilde{x_{in(i)}}}{1}\right)$ is a basis of P_{f_i} as an A_{f_i}-module, in particular it is linearly independent. So we must have $\nu_{ir} = 0$ for any $r = 1, \dots, n(i)$ and $x = y \in M$. This proves that $\mathrm{Ker}((h')_{f_i}) = M$ is finitely generated. Since $\mathrm{Ker}(h')_{f_i} = \mathrm{Ker}((h')_{f_i})$ and this is finitely generated for any $i \in I$, we have that $\mathrm{Ker}(h')$ is also finitely generated, by lemma 2.1.29(3). Notice that $F = \bigoplus_{i\in I} A^{n(i)} \cong A^{\sum_{i\in I} n(i)}$ as A-modules and $\sum_{i\in I} n(i)$ is finite, because I is finite. Let $\varphi : A^{\sum_{i\in I} n(i)} \to F$ be an isomorphism. Then $h' \circ \varphi : A^{\sum_{i\in I} n(i)} \to P$ is a surjective A-linear map, because h' is surjective and A-linear. Moreover, $\mathrm{Ker}(h' \circ \varphi) = \varphi^{-1}(\mathrm{Ker}(h'))$ is isomorphic to $\mathrm{Ker}(h')$ as an A-module, so it is finitely generated, because $\mathrm{Ker}(h')$ is finitely generated. This proves that P is finitely presented (see remark 2.1.26).
Let now M, N be A-modules and $\alpha : M \to N$ a surjective A-linear map. Then $\mathrm{Coker}(\alpha) = 0$. Let $i \in I$ and consider the A_{f_i}-linear map $\alpha_{f_i} : M_{f_i} \to N_{f_i}$. By lemma 2.1.29(2), α_{f_i} is surjective. By assumption, P_{f_i} is free over A_{f_i}, in particular it is projective (example 2.1.11). Then, by lemma 2.1.14 ((i) $\Longrightarrow$ (ii)), we have that the map

$$(\alpha_{f_i})_* : \mathrm{Hom}_{A_{f_i}}(P_{f_i}, M_{f_i}) \to \mathrm{Hom}_{A_{f_i}}(P_{f_i}, N_{f_i}),\ \beta \mapsto \alpha_{f_i} \circ \beta$$

(which is clearly A_{f_i}-linear) is surjective. Since P is finitely presented, by lemma 2.1.27 we have isomorphisms $\varphi_M : \mathrm{Hom}_A(P, M)_{f_i} \to \mathrm{Hom}_{A_{f_i}}(P_{f_i}, M_{f_i})$ and $\varphi_N : \mathrm{Hom}_A(P, N)_{f_i} \to \mathrm{Hom}_{A_{f_i}}(P_{f_i}, N_{f_i})$. Consider the following diagram, where we defined $\alpha_* : \mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N),\ \beta \mapsto \alpha \circ \beta$.

$$\begin{array}{ccc} \mathrm{Hom}_A(P,M)_{f_i} & \xrightarrow{\varphi_M} & \mathrm{Hom}_{A_{f_i}}(P_{f_i}, M_{f_i}) \\ \downarrow{\scriptstyle (\alpha_*)_{f_i}} & & \downarrow{\scriptstyle (\alpha_{f_i})_*} \\ \mathrm{Hom}_A(P,N)_{f_i} & \xrightarrow{\varphi_N} & \mathrm{Hom}_{A_{f_i}}(P_{f_i}, N_{f_i}) \end{array}$$

For any $\frac{\beta}{f_i^m} \in \mathrm{Hom}_A(P, M)_{f_i}$ ($\beta \in \mathrm{Hom}_A(P, M)$ and $m \in \mathbb{N}$) we have that

$$\begin{aligned} \varphi_N\left((\alpha_*)_{f_i}\left(\frac{\beta}{f_i^m}\right)\right) &= \varphi_N\left(\frac{\alpha_*(\beta)}{f_i^m}\right) = \\ &= \varphi_N\left(\frac{\alpha\circ\beta}{f_i^m}\right) = \frac{1}{f_i^m}(\alpha\circ\beta)_{f_i} = \frac{1}{f_i^m}(\alpha_{f_i}\circ\beta_{f_i}) = \\ &= \alpha_{f_i}\circ\left(\frac{\beta_{f_i}}{f_i^m}\right) = (\alpha_{f_i})_*\left(\frac{\beta_{f_i}}{f_i^m}\right) = (\alpha_{f_i})_*\left(\varphi_M\left(\frac{\beta}{f_i^m}\right)\right)\ . \end{aligned}$$

So the diagram commutes, i.e. $\varphi_N \circ (\alpha_*)_{f_i} = (\alpha_{f_i})_* \circ \varphi_M$. Then we have that $(\alpha_*)_{f_i} = \varphi_N^{-1} \circ (\alpha_{f_i})_* \circ \varphi_M$ is surjective, because $(\alpha_{f_i})_*$ is surjective and φ_M and φ_N are isomorphisms. Since this holds for any $i \in I$, we have that α_* is surjective, by lemma 2.1.29. By lemma 2.1.14 ((ii) $\Longrightarrow$ (i)), we have that P is projective.

□

Remark 2.1.31. The proposition 2.1.30 has an important geometrical meaning: it means that P is finitely generated and projective if and only if the associated sheaf of $\mathcal{O}_{\mathrm{Spec}(A)}$-modules $\widetilde{P}$ is locally free of finite rank (recall that, given a scheme $(X, \mathcal{O}_X)$ and a sheaf $\mathcal{F}$ of $\mathcal{O}_X$-modules, $\mathcal{F}$ is *locally free of finite rank* if for every $x \in X$ there exists an open neighbourhood U of x in X such that $\mathcal{F}_{|U} \cong \bigoplus_{i=1}^{n_U} (\mathcal{O}_X)_{|U}$ as sheaves of $(\mathcal{O}_X)_{|U}$-modules, for an $n_U \in \mathbb{N}$).
Indeed, if P is finitely generated and projective, let $(f_i)_{i\in I}$ be a collection of elements of A as in 2.1.30(iv). Let $\mathfrak{p} \in \mathrm{Spec}(A)$. Then $\mathfrak{p} \neq A$, so there exists $i_0 \in I$ such that $f_{i_0} \notin \mathfrak{p}$ (otherwise we would have $A = \sum_{i\in I} f_i A \subseteq \mathfrak{p}$). This means that $\mathfrak{p} \in \mathrm{D}(f_{i_0})$, i.e. the distinguished open subset $\mathrm{D}(f_{i_0})$ is an open neighbourhood of $\mathfrak{p}$ in $\mathrm{Spec}(A)$. Consider the sheaf of $\mathcal{O}_{\mathrm{Spec}(A_{f_{i_0}})}$-modules $\widetilde{P_{f_{i_0}}}$. By assumption, $P_{f_{i_0}}$ is a free $A_{f_{i_0}}$-module, so there exists $n \in \mathbb{N}$ such that $P_{f_{i_0}} \cong A_{f_{i_0}}^n$ as $A_{f_{i_0}}$-modules. Then

$$\widetilde{P_{f_{i_0}}} \cong \widetilde{A_{f_{i_0}}^n} \cong \bigoplus_{i=1}^{n} \widetilde{A_{f_{i_0}}} = \bigoplus_{i=1}^{n} \mathcal{O}_{\mathrm{Spec}(A_{f_{i_0}})} ,$$

as sheaves of $\mathcal{O}_{\mathrm{Spec}(A_{f_{i_0}})}$-modules. Moreover, we have that

$$\Big(\mathrm{D}(f_{i_0}), (\mathcal{O}_{\mathrm{Spec}(A)})_{|\mathrm{D}(f_{i_0})}\Big) \cong \mathrm{Spec}(A_{f_{i_0}}) .$$

This isomorphism allows us to see $\widetilde{P_{f_{i_0}}}$ as a sheaf of $(\mathcal{O}_{\mathrm{Spec}(A)})_{|\mathrm{D}(f_{i_0})}$-modules on $\mathrm{D}(f_{i_0})$ and it can be easily proved that this sheaf is isomorphic to $\widetilde{P}_{|\mathrm{D}(f_{i_0})}$. Then we get that $\widetilde{P}_{|\mathrm{D}(f_{i_0})} \cong \bigoplus_{i=1}^{n} (\mathcal{O}_{\mathrm{Spec}(A)})_{|\mathrm{D}(f_{i_0})}$. So $\widetilde{P}$ is locally free of finite rank.
Conversely, assume that $\widetilde{P}$ is locally free of finite rank and let $\mathfrak{p}$ be a prime ideal of A, i.e. $\mathfrak{p} \in \mathrm{Spec}(A)$. Then there exists an open neighbourhood U of $\mathfrak{p}$ in $\mathrm{Spec}(A)$ such that $\widetilde{P}_{|U} \cong \bigoplus_{i=1}^{n_U} (\mathcal{O}_{\mathrm{Spec}(A)})_{|U}$ as sheaves of $(\mathcal{O}_{\mathrm{Spec}(A)})_{|U}$-modules. Consider now the stalks at $\mathfrak{p}$. We have that $((\mathcal{O}_{\mathrm{Spec}(A)})_{|U})_{\mathfrak{p}} \cong (\mathcal{O}_{\mathrm{Spec}(A)})_{\mathfrak{p}} \cong A_{\mathfrak{p}}$. Then we have isomorphisms of $A_{\mathfrak{p}}$-modules

$$P_{\mathfrak{p}} \cong \left(\widetilde{P}\right)_{\mathfrak{p}} \cong \left(\widetilde{P}_{|U}\right)_{\mathfrak{p}} \cong \left(\bigoplus_{i=1}^{n_U} (\mathcal{O}_{\mathrm{Spec}(A)})_{|U}\right)_{\mathfrak{p}} \cong \bigoplus_{i=1}^{n_U} ((\mathcal{O}_{\mathrm{Spec}(A)})_{|U})_{\mathfrak{p}} \cong \bigoplus_{i=1}^{n_U} A_{\mathfrak{p}}$$

(we used the fact that stalks commute with direct sums). So $P_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of finite rank (this is also part of the statement of corollary 2.1.33 and we will give an alternative proof with an algebraic approach). Then the condition (ii) of the proposition 2.1.30 is satisfied and P must be finitely generated and projective.

Corollary 2.1.32. *Let P be an A-module. If there exists a collection $(f_i)_{i\in I}$ of elements of A such that $\sum_{i\in I} f_i A = A$ and for every $i \in I$ the A_{f_i}-module P_{f_i} is finitely generated and projective, then P is finitely generated and projective as an A-module.*

Proof. Let $i \in I$. Since P_{f_i} is finitely generated and projective over A_{f_i}, by proposition 2.1.30 ((i) $\Longrightarrow$ (iv)) there exists a collection $(\alpha_{ij})_{j\in J_i}$ of elements of A_{f_i} such that $\sum_{j\in J_i} \alpha_{ij} A_{f_i} = A_{f_i}$ and the $(A_{f_i})_{\alpha_{ij}}$-module $(P_{f_i})_{\alpha_{ij}}$ is free of finite rank. Let $j \in J_i$. By definition of localization, there exist $h_{ij} \in A$ and $n_{ij} \in \mathbb{N}$ such that $\alpha_{ij} = \frac{h_{ij}}{f_i^{n_{ij}}}$. Define

$$\varphi : A_{f_i h_{ij}} \to (A_{f_i})_{\alpha_{ij}},\ \frac{x}{(f_i h_{ij})^n} \mapsto \frac{\left(\frac{x}{f_i^{n(1+n_{ij})}}\right)}{\alpha_{ij}^n}.$$

Let us check that φ is well defined. If $\frac{x}{(f_i h_{ij})^n} = \frac{y}{(f_i h_{ij})^m}$, with $x, y \in A$ and $n, m \in \mathbb{N}$, then there exists $k \in \mathbb{N}$ such that $(f_i h_{ij})^k (x(f_i h_{ij})^m - y(f_i h_{ij})^n) = 0$. Then in A_{f_i} we have

$$\begin{aligned} 0 = \frac{(f_i h_{ij})^k (x(f_i h_{ij})^m - y(f_i h_{ij})^n)}{f_i^{(k+m+n)(1+n_{ij})}} &= \\ = \frac{f_i^k h_{ij}^k}{f_i^{k(1+n_{ij})}} \left(\frac{x f_i^m h_{ij}^m}{f_i^{(m+n)(1+n_{ij})}} - \frac{y f_i^n h_{ij}^n}{f_i^{(m+n)(1+n_{ij})}} \right) &= \\ = \left(\frac{h_{ij}}{f_i^{n_{ij}}}\right)^k \left(\frac{x}{f_i^{n(1+n_{ij})}} \left(\frac{h_{ij}}{f_i^{n_{ij}}}\right)^m - \frac{y}{f_i^{m(1+n_{ij})}} \left(\frac{h_{ij}}{f_i^{n_{ij}}}\right)^n \right) &= \\ = \alpha_{ij}^k \left(\frac{x}{f_i^{n(1+n_{ij})}} \alpha_{ij}^m - \frac{y}{f_i^{m(1+n_{ij})}} \alpha_{ij}^n \right) \end{aligned}$$

So

$$\frac{\left(\frac{x}{f_i^{n(1+n_{ij})}}\right)}{\alpha_{ij}^n} = \frac{\left(\frac{y}{f_i^{m(1+n_{ij})}}\right)}{\alpha_{ij}^m}$$

in $(A_{f_i})_{\alpha_{ij}}$ and this proves that φ is well defined. Moreover, we have that

$$\varphi\left(1_{A_{f_i h_{ij}}}\right) = \varphi\left(\frac{1}{(f_i h_{ij})^0}\right) = \frac{\left(\frac{1}{f_i^0}\right)}{\alpha_{ij}^0} = 1_{(A_{f_i})_{\alpha_{ij}}}$$

and for every $x, y \in A$, $n, m \in \mathbb{N}$ we have

$$\begin{aligned} \varphi\left(\frac{x}{(f_i h_{ij})^n} \frac{y}{(f_i h_{ij})^m}\right) = \varphi\left(\frac{xy}{(f_i h_{ij})^{n+m}}\right) &= \\ = \frac{\left(\frac{xy}{f_i^{(n+m)(1+n_{ij})}}\right)}{\alpha_{ij}^{n+m}} = \frac{\left(\frac{x}{f_i^{n(1+n_{ij})}} \frac{y}{f_i^{m(1+n_{ij})}}\right)}{\alpha_{ij}^n \alpha_{ij}^m} &= \\ = \frac{\left(\frac{x}{f_i^{n(1+n_{ij})}}\right)}{\alpha_{ij}^n} \frac{\left(\frac{y}{f_i^{m(1+n_{ij})}}\right)}{\alpha_{ij}^m} = \varphi\left(\frac{x}{(f_i h_{ij})^n}\right) \varphi\left(\frac{y}{(f_i h_{ij})^m}\right) \end{aligned}$$

and

$$\varphi\left(\frac{x}{(f_ih_{ij})^n}+\frac{y}{(f_ih_{ij})^m}\right)=\varphi\left(\frac{x(f_ih_{ij})^m+y(f_ih_{ij})^n)}{(f_ih_{ij})^{n+m}}\right)=$$
$$=\frac{\left(\frac{x(f_ih_{ij})^m+y(f_ih_{ij})^n}{f_i^{(n+m)(1+n_{ij})}}\right)}{\alpha_{ij}^{n+m}}=\frac{\left(\frac{x}{f_i^{n(1+n_{ij})}}\left(\frac{h_{ij}}{f_i^{n_{ij}}}\right)^m+\frac{y}{f_i^{m(1+n_{ij})}}\left(\frac{h_{ij}}{f_i^{n_{ij}}}\right)^n\right)}{\alpha_{ij}^n\alpha_{ij}^m}=$$
$$=\frac{\left(\frac{x}{f_i^{n(1+n_{ij})}}\alpha_{ij}^m+\frac{y}{f_i^{m(1+n_{ij})}}\alpha_{ij}^n\right)}{\alpha_{ij}^n\alpha_{ij}^m}=\frac{\left(\frac{x}{f_i^{n(1+n_{ij})}}\right)}{\alpha_{ij}^n}+\frac{\left(\frac{y}{f_i^{m(1+n_{ij})}}\right)}{\alpha_{ij}^m}=$$
$$=\varphi\left(\frac{x}{(f_ih_{ij})^n}\right)+\varphi\left(\frac{y}{(f_ih_{ij})^m}\right).$$

Then φ is a ring homomorphism. Let now $\frac{x}{(f_ih_{ij})^n}\in\mathrm{Ker}(\varphi)$, with $x\in A$ and $n\in\mathbb{N}$. This means that

$$\frac{\left(\frac{x}{f_i^{n(1+n_{ij})}}\right)}{\alpha_{ij}^n}=\varphi\left(\frac{x}{(f_ih_{ij})^n}\right)=0\,.$$

Then there exists $k\in\mathbb{N}$ such that $\alpha_{ij}^k\frac{x}{f_i^{n(1+n_{ij})}}=0$ in A_{f_i}, i.e. $\frac{h_{ij}^kx}{f_i^{kn_{ij}+n(1+n_{ij})}}=\left(\frac{h_{ij}}{f_i^{n_{ij}}}\right)^k\frac{x}{f_i^{n(1+n_{ij})}}=0$. This means that there exists $m\in\mathbb{N}$ such that $f_i^mh_{ij}^kx=0$. Let $K:=\max\{k,m\}$. Then

$$(f_ih_{ij})^Kx=f_i^Kh_{ij}^Kx=f_i^{K-m}h_{ij}^{K-k}f_i^mh_{ij}^kx=0\,.$$

So $\frac{x}{(f_ih_{ij})^n}=0$ in $A_{f_ih_{ij}}$. Then $\mathrm{Ker}(\varphi)=0$, i.e. φ is injective.

Let now $\frac{\left(\frac{x}{f_i^n}\right)}{\alpha_{ij}^m}\in(A_{f_i})_{\alpha_{ij}}$, with $x\in A$, $n,m\in\mathbb{N}$. Let $k:=\max\{m,n-mn_{ij}\}\in\mathbb{N}$ and consider $\frac{xf_i^{k-(n-mn_{ij})}h_{ij}^{k-m}}{(f_ih_{ij})^k}\in A_{f_ih_{ij}}$. We have that

$$\varphi\left(\frac{xf_i^{k-(n-mn_{ij})}h_{ij}^{k-m}}{(f_ih_{ij})^k}\right)=\frac{\left(\frac{xf_i^{k-(n-mn_{ij})}h_{ij}^{k-m}}{f_i^{k(1+n_{ij})}}\right)}{\alpha_{ij}^k}=\frac{\left(\frac{xh_{ij}^{k-m}}{f_i^{kn_{ij}+n-mn_{ij}}}\right)}{\alpha_{ij}^k}=$$
$$=\frac{\left(\frac{x}{f_i^n}\left(\frac{h_{ij}}{f_i^{n_{ij}}}\right)^{k-m}\right)}{\alpha_{ij}^k}=\frac{\left(\frac{x}{f_i^n}\alpha_{ij}^{k-m}\right)}{\alpha_{ij}^k}=\frac{\left(\frac{x}{f_i^n}\right)}{\alpha_{ij}^m}\,.$$

This proves that φ is surjective. So $\varphi:A_{f_ih_{ij}}\to(A_{f_i})_{\alpha_{ij}}$ is an isomorphism. Then we can see the $(A_{f_i})_{\alpha_{ij}}$-module $(P_{f_i})_{\alpha_{ij}}$ as an $A_{f_ih_{ij}}$-module, which is again free of finite rank. It can then be proved that $P_{f_ih_{ij}}\cong(P_{f_i})_{\alpha_{ij}}$ as $A_{f_ih_{ij}}$-modules (the proof

is analogous to what we did above for $A_{f_i h_{ij}}$ and $(A_{f_i})_{\alpha_{ij}})$. So $P_{f_i h_{ij}}$ is a free $A_{f_i h_{ij}}$-module of finite rank.
Now, since $\sum_{j\in J_i} \alpha_{ij} A_{f_i} = A_{f_i}$, there exist $\lambda_{ij} = \frac{s_{ij}}{f_i^{m_{ij}}} \in A_{f_i}$ (with $s_{ij} \in A$, $m_{ij} \in \mathbb{N}$, for any $j \in J_i$) such that $\frac{1}{1} = \sum_{j\in J_i} \alpha_{ij}\lambda_{ij} = \sum_{j\in J_i} \frac{h_{ij}}{f_i^{n_{ij}}}\frac{s_{ij}}{f_i^{m_{ij}}} = \sum_{j\in J_i} \frac{h_{ij}s_{ij}}{f_i^{n_{ij}+m_{ij}}}$. Let $N := \max_{j\in J_i}(n_{ij}+m_{ij})$. Then

$$\frac{1}{1} = \sum_{j\in J_i} \frac{h_{ij}}{f_i^{n_{ij}}}\frac{s_{ij}}{f_i^{m_{ij}}} = \sum_{j\in J_i} \frac{h_{ij}s_{ij}}{f_i^{n_{ij}+m_{ij}}} = \frac{\sum_{j\in J_i} h_{ij}s_{ij}f_i^{N-n_{ij}-m_{ij}}}{f_i^N} ,$$

which means that there exists $k \in \mathbb{N}$ such that

$$0 = f_i^k \left(1 \cdot f_i^N - 1 \cdot \sum_{j\in J_i} h_{ij}s_{ij}f_i^{N-n_{ij}-m_{ij}} \right) = f_i^{k+N} - \sum_{j\in J_i} h_{ij}s_{ij}f_i^{k+N-n_{ij}-m_{ij}} ,$$

i.e. $f_i^{k+N} = \sum_{j\in J_i} h_{ij}s_{ij}f_i^{k+N-n_{ij}-m_{ij}}$. Let $\mathfrak{m}$ be a maximal ideal of A. Since $\sum_{i\in I} f_iA = A$, there exists $i \in I$ such that $f_i \notin \mathfrak{m}$ (otherwise $A \subseteq \mathfrak{m}$, which is a contradiction). Since $\mathfrak{m}$ is maximal, it is in particular prime. Then $f_i^h \notin \mathfrak{m}$ for any $h > 0$. In particular, $f_i^{k+N+1} \notin \mathfrak{m}$. Then $\sum_{i\in I} f_i^{k+N+1}A \nsubseteq \mathfrak{m}$. Since this holds for every maximal ideal $\mathfrak{m}$, we must have that $\sum_{i\in I} f_i^{k+N+1}A = A$. Then there exist $a_i \in A$ (for $i \in I$) such that

$$1 = \sum_{i\in I} f_i^{k+N+1}a_i = \sum_{i\in I} f_i \left(\sum_{j\in J_i} h_{ij}s_{ij}f_i^{k+N-n_{ij}-m_{ij}} \right) a_i =$$
$$= \sum_{i\in I}\sum_{j\in J_i} f_ih_{ij}s_{ij}f_i^{k+N-n_{ij}-m_{ij}}a_i \in \sum_{\substack{i\in I\\ j\in J_i}} (f_ih_{ij})A .$$

Then $\sum_{i\in I, j\in J}(f_ih_{ij})A = A$, because $\sum_{i\in I, j\in J}(f_ih_{ij})A$ is an ideal of A. So the collection $(f_ih_{ij})_{i\in I, j\in J_i}$ satisfies the assumptions of proposition 2.1.30 ((iv) $\Longrightarrow$ (i)), which allows us to conclude that P is a finitely generated and projective A-module ☐

Corollary 2.1.33. *Let P be a finitely generated projective A-module.*

(1) For any prime ideal $\mathfrak{p}$ of A, we have that $P_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module of finite rank.

(2) The function $\mathrm{rank}_A(P) : \mathrm{Spec}(A) \to \mathbb{Z}$, $\mathfrak{p} \mapsto \mathrm{rank}_{A_\mathfrak{p}}(P_\mathfrak{p})$ *is locally constant. In particular, it is continuous (if we endow $\mathbb{Z}$ with the discrete topology) and if* $\mathrm{Spec}(A)$ *is connected it is constant.*

Proof. Since P is finitely generated and projective, by the implication (i) $\Longrightarrow$ (iv) of the proposition 2.1.30 there exists a collection $(f_i)_{i\in I}$ of elements of A such that $\sum_{i\in I} f_iA = A$ and for each $i \in I$ the A_{f_i}-module P_{f_i} is free of finite rank.

(1) Let $\mathfrak{p}$ be a prime ideal of A. In particular, $P \neq A$. Then there exists $i \in I$ such that $f_i \notin \mathfrak{p}$ (otherwise we would have $A = \sum_{i \in I} f_i A \subseteq \mathfrak{p}$). Since $\mathfrak{p}$ is prime, it follows that $f_i^n \notin \mathfrak{p}$ for any $n \in \mathbb{N}$, i.e. $S_{f_i} \subseteq A \backslash \mathfrak{p}$. Then we have that $A_\mathfrak{p} \cong (A_{f_i})_{\mathfrak{p}_{f_i}}$. This isomorphism allows us to see $(P_{f_i})_{\mathfrak{p}_{f_i}}$ as an $A_\mathfrak{p}$-module. Then $P_\mathfrak{p} \cong (P_{f_i})_{\mathfrak{p}_{f_i}}$ as $A_\mathfrak{p}$-modules. By assumption P_{f_i} is free of finite rank, i.e. there exists $n \in \mathbb{N}$ such that $P_{f_i} \cong (A_{f_i})^n$ as A_{f_i}-modules. Since the localization commutes with direct sums, we get that $P_\mathfrak{p} \cong (P_{f_i})_{\mathfrak{p}_{f_i}} \cong ((A_{f_i})_{\mathfrak{p}_{f_i}})^n \cong A_\mathfrak{p}^n$ as $A_\mathfrak{p}$-modules. This proves the claim.

(2) Let $\mathfrak{p} \in \mathrm{Spec}(A)$ and i as in the proof of point (1). Then $\mathrm{D}(f_i)$ is an open neighbourhood of $\mathfrak{p}$ in $\mathrm{Spec}(A)$. If $n \in \mathbb{N}$ is such that $P_{f_i} \cong (A_{f_i})^n$ as A_{f_i}-modules, in the proof of point (1) we saw that $P_\mathfrak{p} \cong A_\mathfrak{p}^n$ and so $\mathrm{rank}_{A_\mathfrak{p}}(P_\mathfrak{p}) = n$ (notice that this rank is well defined because $A_\mathfrak{p} \neq 0$, since $\frac{1}{1} \neq \frac{0}{1}$). Let now $\mathfrak{q} \in \mathrm{D}(f_i)$. This means that $f_i \notin \mathfrak{q}$. Then we can apply the same argument we used in point (1) in order to show that $\mathrm{rank}_{A_\mathfrak{q}}(P_\mathfrak{q}) = n$. Hence the function $\mathrm{rank}_A(P)$ is locally constant. The rest of the statement follows immediately, because a locally constant function is always continuous and a continuous function from a connected space to a discrete one must be constant.

□

Remark 2.1.34. Let $(X, \mathcal{O}_X)$ be a scheme. Working with stalks, one can associate a rank function $X \to \mathbb{Z}$ to any locally free sheaf of $\mathcal{O}_X$-modules of finite rank and this function is locally constant. Then corollary 2.1.33 can be seen as a consequence of remark 2.1.31.

Definition 2.1.35. Let P be a finitely generated projective A-module.

(1) The function $\mathrm{rank}_A(P) : \mathrm{Spec}(A) \to \mathbb{Z}$, $\mathfrak{p} \mapsto \mathrm{rank}_{A_\mathfrak{p}}(P_\mathfrak{p})$ defined in corollary 2.1.33(2) is called the *rank* of P over A.

(2) We say that P is *faithfully projective* if $\mathrm{rank}_A(P)(\mathfrak{p}) \geq 1$ for every $\mathfrak{p} \in \mathrm{Spec}(A)$ (we will write shortly $\mathrm{rank}_A(P) \geq 1$).

Remark 2.1.36. (1) Recall that any free module is projective (example 2.1.11). So now we have two definitions of rank in the case of a finitely generated free module (remark 2.1.2 and definition 2.1.35(1)). The first definition gives us a non-negative integer, while the second one is a function from $\mathrm{Spec}(A)$ to $\mathbb{Z}$. However, if P is a free A-module of rank n ($n \in \mathbb{N}$), then $P_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module of rank n for any $\mathfrak{p} \in \mathrm{Spec}(A)$, because the localization commutes with direct sum. So the rank function we defined in 2.1.35(1) is constantly equal to n, namely to the rank defined as in 2.1.2.

(2) Notice that, unlike the definition of the rank of a finitely generated A-module that we gave in remark 2.1.2, the definition we gave in 2.1.35(1) makes sense also when $A = 0$. Indeed, in that case we have that $\mathrm{Spec}(A) = \emptyset$ and the rank of 0 (the unique A-module) is the unique function $\emptyset \to \mathbb{Z}$.

The rank enjoys a lot of interesting properties concerning operations between finitely generated projective A-modules. As an example, we see what happens with direct sums and with tensor products (the results are intuitive if we think about the case of free modules of finite rank).

Lemma 2.1.37. *Let $P_1, \dots, P_n$ be finitely generated projective A-modules. Then $\bigoplus_{i=1}^n P_i$ is also finitely genererated and projective over A and*

$$\mathrm{rank}_A\left(\bigoplus_{i=1}^n P_i\right) = \sum_{i=1}^n \mathrm{rank}_A(P_i)$$

as functions on $\mathrm{Spec}(A)$ *(i.e.* $\mathrm{rank}_A\left(\bigoplus_{i=1}^n P_i\right)(\mathfrak{p}) = \sum_{i=1}^n \mathrm{rank}_A(P_i)(\mathfrak{p})$ *for any* $\mathfrak{p} \in \mathrm{Spec}(A)$*).*

Proof. Since P_i is projective for every $i \in I$, we have that $\bigoplus_{i=1}^n P_i$ is projective by corollary 2.1.10. Moreover, if $(v_{i1}, \dots, v_{im_i})$ generates P_i for any $i = 1, \dots, n$, then $((v_{1k_1}, \dots, v_{nk_n}))_{k_1=1,\dots,m_1,\dots,k_n=1,\dots,m_n}$ generates $\bigoplus_{i=1}^n P_i$. Indeed, if $(x_1, \dots, x_n) \in \bigoplus_{i=1}^n P_i$, then for every $i = 1, \dots, n$ we have that $x_i \in P_i$ and so there exist $\lambda_{i1}, \dots, \lambda_{im_i} \in A$ such that $x_i = \sum_{k_i=1}^{m_i} \lambda_{ik_i} v_{ik_i}$. So

$$(x_1, \dots, x_n) = \left(\sum_{k_1=1}^{m_1} \lambda_{1k_1} v_{1k_1}, \dots, \sum_{k_n=1}^{m_n} \lambda_{nk_n} v_{nk_n}\right) = $$
$$= \sum_{k_1=1}^{m_1} \cdots \sum_{k_n=1}^{m_n} \lambda_{1k_1} \cdots \lambda_{nk_n} (v_{1k_1}, \dots, v_{nk_n}) \, .$$

This shows that $\bigoplus_{i=1}^n P_i$ is finitely generated.
Let now $\mathfrak{p} \in \mathrm{Spec}(A)$. Fix $i \in I$. By corollary 2.1.33(1), we have that $(P_i)_\mathfrak{p}$ is free of finite rank. Define $m_i := \mathrm{rank}_{A_\mathfrak{p}}((P_i)_\mathfrak{p})$ (by definition of $\mathrm{rank}_A(P_i)$, this means that $m_i = \mathrm{rank}_A(P_i)(\mathfrak{p})$). Then $(P_i)_\mathfrak{p} \cong A_\mathfrak{p}^{m_i}$. Since the localization commutes with direct sums (see lemma 2.1.19, recalling that localization at $\mathfrak{p}$ corresponds to tensor product with $A_\mathfrak{p}$), we have that

$$\left(\bigoplus_{i=1}^n P_i\right)_\mathfrak{p} \cong \bigoplus_{i=1}^n (P_i)_\mathfrak{p} \cong \bigoplus_{i=1}^n A_\mathfrak{p}^{m_i} \cong A_\mathfrak{p}^{\sum_{i=1}^n m_i}$$

as $A_\mathfrak{p}$-modules (notice that lemma 2.1.19 gives only an isomorphism of A-modules, but it is immediate to check that in this case that isomorphism is also $A_\mathfrak{p}$-linear). Then, by definition of the rank for finitely generated projective A-modules, we get that

$$\mathrm{rank}_A\left(\bigoplus_{i=1}^n P_i\right)(\mathfrak{p}) = \sum_{i=1}^n m_i = \sum_{i=1}^n \mathrm{rank}_A(P_i)(\mathfrak{p}) \, .$$

□

Lemma 2.1.38. *Localization and tensor products commute. More precisely, if S is a multiplicatively closed subset of A and M, N are A-modules, then $S^{-1}(M \otimes_A N) \cong (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N)$ as $S^{-1}A$-modules.*

Proof. Consider the map

$$\varphi : S^{-1}M \times S^{-1}N \to S^{-1}(M \otimes_A N),\ \left(\frac{m}{s}, \frac{n}{t}\right) \mapsto \frac{m \otimes n}{st} .$$

First of all we check that φ is well defined. Assume that $m_1, m_2 \in M$, $n_1, n_2 \in N$ and $s_1, s_2, t_1, t_2 \in S$ are such that $\frac{m_1}{s_1} = \frac{m_2}{s_2}$ and $\frac{n_1}{t_1} = \frac{n_2}{t_2}$. Then there exist $u, v \in S$ such that $u(m_1 s_2 - m_2 s_1) = 0$ and $v(n_1 t_2 - n_2 t_1) = 0$. Then $uv \in S$ and

$$\begin{aligned} uv(s_2 t_2(m_1 \otimes n_1) - s_1 t_1(m_2 \otimes n_2)) = (um_1 s_2) \otimes (vn_1 t_2) - (um_2 s_1) \otimes (vn_2 s_1) = \\ = (um_2 s_1) \otimes (vn_2 t_1) - (um_2 s_1) \otimes (vn_2 s_1) = 0 . \end{aligned}$$

So $\frac{m_1 \otimes n_1}{s_1 t_1} = \frac{m_2 \otimes n_2}{s_2 t_2}$. This proves that φ is well defined. We prove now that φ is $S^{-1}A$-bilinear. Let $\lambda_1 = \frac{a_1}{u_1}, \lambda_2 = \frac{a_2}{u_2} \in S^{-1}A$, $\frac{m_1}{s_1}, \frac{m_2}{s_2} \in S^{-1}M$ and $\frac{n}{t} \in S^{-1}N$. Then

$$\begin{aligned} &\varphi\left(\lambda_1 \frac{m_1}{s_1} + \lambda_2 \frac{m_2}{s_2}, \frac{n}{t}\right) = \varphi\left(\frac{u_2 s_2 a_1 m_1 + u_1 s_1 a_2 m_2}{s_1 s_2 u_1 u_2}, \frac{n}{t}\right) = \\ &= \frac{(u_2 s_2 a_1 m_1 + u_1 s_1 a_2 m_2) \otimes n}{s_1 s_2 u_1 u_2 t} = \frac{u_2 s_2 a_1 (m_1 \otimes n) + u_1 s_1 a_2 (m_2 \otimes n)}{s_1 s_2 u_1 u_2 t} = \\ &= \frac{a_1}{u_1} \frac{m_1 \otimes n}{s_1 t} + \frac{a_2}{u_2} \frac{m_2 \otimes n}{s_2 t} = \lambda_1 \varphi\left(\frac{m_1}{s_1}, \frac{n}{t}\right) + \lambda_2 \varphi\left(\frac{m_2}{s_2}, \frac{n}{t}\right) . \end{aligned}$$

Analogously, if $\lambda_1 = \frac{a_1}{u_1}, \lambda_2 = \frac{a_2}{u_2} \in S^{-1}A$, $\frac{m}{s} \in S^{-1}M$ and $\frac{n_1}{t_1}, \frac{n_2}{t_2} \in S^{-1}N$, we have that

$$\begin{aligned} &\varphi\left(\frac{m}{s}, \lambda_1 \frac{n_1}{t_1} + \lambda_2 \frac{n_2}{t_2}\right) = \varphi\left(\frac{m}{s}, \frac{u_2 t_2 a_1 n_1 + u_1 t_1 a_2 n_2}{t_1 t_2 u_1 u_2}\right) = \\ &= \frac{(u_2 s_2 a_1 m_1 + u_1 s_1 a_2 m_2) \otimes n}{s_1 s_2 u_1 u_2 t} = \frac{u_2 t_2 a_1 (m \otimes n_1) + u_1 t_1 a_2 (m \otimes n_2)}{s u_1 u_2 t_1 t_2} = \\ &= \frac{a_1}{u_1} \frac{m \otimes n_1}{s t_1} + \frac{a_2}{u_2} \frac{m \otimes n_2}{s t_2} = \lambda_1 \varphi\left(\frac{m}{s}, \frac{n_1}{t_1}\right) + \lambda_2 \varphi\left(\frac{m}{s}, \frac{n_2}{t_2}\right) . \end{aligned}$$

So φ is $S^{-1}A$-bilinear. By the universal property of the tensor product, φ induces an $S^{-1}A$-linear map $\Phi : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$ with $\Phi\left(\frac{m}{s} \otimes \frac{n}{t}\right) = \varphi\left(\left(\frac{m}{s}, \frac{n}{t}\right)\right)$ for any $\frac{m}{s} \in S^{-1}M$, $\frac{n}{t} \in S^{-1}N$.
The map $\psi : M \times N \to (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N)$, $(m, n) \mapsto \frac{m}{1} \otimes \frac{n}{1}$ is clearly A-bilinear, so it induces an A-linear map $\Psi : M \otimes_A N \to (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N)$ with $\Psi(m \otimes n) = \psi((m, n)) = \frac{m}{1} \otimes \frac{n}{1}$ for any $m \in M$, $n \in N$. Define

$$\Psi' : S^{-1}(M \otimes_A N) \to (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N),\ \frac{x}{s} \mapsto \frac{1}{s}\Psi(x) .$$

Let us check that Ψ' is well defined. Let $x_1, x_2 \in M \otimes_A N$, $s_1, s_2 \in S$ such that $\frac{x_1}{s_1} = \frac{x_2}{s_2}$. Then there exists $u \in S$ such that $u(x_1 s_2 - x_2 s_1) = 0$. Since Ψ is A-linear it follows that $0 = \Psi(u x_1 s_2 - u x_2 s_1) = u s_2 \Psi(x_1) - u s_1 \Psi(x_2)$. So $\frac{1}{s_1}\Psi(x_1) = \frac{1}{u s_1 s_2}(u s_2 \Psi(x_1)) = \frac{1}{u s_1 s_2}(u s_1 \Psi(x_2)) = \frac{1}{s_2}\Psi(x_2)$. This proves that Ψ' is well defined.

We prove now that Ψ' is $S^{-1}A$-linear. Let $\lambda_1 = \frac{a_1}{u_1}, \lambda_2 = \frac{a_2}{u_2} \in S^{-1}A$, $\frac{x_1}{s_1}, \frac{x_2}{s_2} \in S^{-1}(M \otimes_A N)$. Since Ψ is A-linear, we have that

$$\Psi'\left(\lambda_1 \frac{x_1}{s_1} + \lambda_2 \frac{x_2}{s_2}\right) = \Psi'\left(\frac{u_2 s_2 a_1 x_1 + u_1 s_1 a_2 x_2}{u_1 u_2 s_1 s_2}\right) =$$
$$= \frac{1}{u_1 u_2 s_1 s_2}\Psi(u_2 s_2 a_1 x_1 + u_1 s_1 a_2 x_2) = \frac{1}{u_1 u_2 s_1 s_2}(u_2 s_2 a_1 \Psi(x_1) + u_1 s_1 a_2 \Psi(x_2)) =$$
$$= \frac{a_1}{u_1}\frac{1}{s_1}\Psi(x_1) + \frac{a_2}{u_2}\frac{1}{s_2}\Psi(x_2) = \lambda_1 \Psi'\left(\frac{x_1}{s_1}\right) + \lambda_2 \Psi'\left(\frac{x_2}{s_2}\right) .$$

So Ψ' is $S^{-1}A$-linear. It remains to prove that Φ and Ψ' are inverse to each other. For any $\frac{m}{s} \in S^{-1}M$, $\frac{n}{t} \in S^{-1}N$, we have

$$(\Psi' \circ \Phi)\left(\frac{m}{s} \otimes \frac{n}{t}\right) = \Psi'\left(\frac{m \otimes n}{st}\right) = \frac{1}{st}\Psi(m \otimes n) =$$
$$= \frac{1}{st}\frac{m}{1} \otimes \frac{n}{1} = \frac{m}{s} \otimes \frac{n}{t} = \mathrm{id}_{(S^{-1}M)\otimes_{S^{-1}A}(S^{-1}N)}\left(\frac{m}{s} \otimes \frac{n}{t}\right) .$$

So $\Psi' \circ \Phi = \mathrm{id}_{(S^{-1}M)\otimes_{S^{-1}A}(S^{-1}N)}$ (by linearity, it is enough to check equality on pure tensors). Conversely, notice that $S^{-1}(M \otimes_A N)$ is generated by elements of the form $\frac{m \otimes n}{s}$, with $m \in M$, $n \in N$ and $s \in S$. We have that

$$(\Phi \circ \Psi')\left(\frac{m \otimes n}{s}\right) = \Phi\left(\frac{1}{s}\Psi(m \otimes n)\right) = \Phi\left(\frac{1}{s}\frac{m}{1} \otimes \frac{n}{1}\right) =$$
$$= \Phi\left(\frac{m}{s} \otimes \frac{n}{1}\right) = \frac{m \otimes n}{s} = \mathrm{id}_{S^{-1}(M \otimes_A N)}\left(\frac{m \otimes n}{s}\right)$$

for any $m \in M$, $n \in N$ and $s \in S$. So $\Phi \circ \Psi' = \mathrm{id}_{S^{-1}(M \otimes_A N)}$. This ends the proof. ☐

Lemma 2.1.39. *If P and P' are projective A-modules, we have that $P \otimes_A P'$ is also projective.*

Proof. Since P and P' are projective, by lemma 2.1.14 ((i) $\implies$ (iv)) there exist two A-modules Q and Q' such that $P \oplus Q$ and $P' \oplus Q'$ are free. Then there exist two index sets I and J such that $P \oplus Q \cong \bigoplus_{i \in I} A$ and $P' \oplus Q' \cong \bigoplus_{j \in J} A$. Since the tensor product commutes with direct sums (lemma 2.1.19, notice that this works with both factors, because for any two A-modules M, N we have that $M \otimes_A N \cong N \otimes_A M$), we have that

$$\bigoplus_{\substack{i \in I \\ j \in J}} A \cong \bigoplus_{\substack{i \in I \\ j \in J}} A \otimes_A A \cong \left(\bigoplus_{i \in I} A\right) \otimes_A \left(\bigoplus_{j \in J} A\right) \cong (P \oplus Q) \otimes_A (P' \oplus Q') \cong$$
$$\cong (P \otimes_A P') \oplus (P \otimes_A Q') \oplus (Q \otimes_A P') \oplus (Q \otimes_A Q') .$$

Then, if we define $R := (P \otimes_A Q') \oplus (Q \otimes_A P') \oplus (Q \otimes_A Q')$, we have that $(P \otimes_A P') \oplus R \cong \bigoplus_{i \in I, j \in J} A$ is free. Hence $P \otimes_A P'$ is projective by lemma 2.1.14 ((iv) $\implies$ (i)). ☐

Lemma 2.1.40. *Let P and P' be finitely generated projective A-modules. Then $P \otimes_A P'$ is also finitely generated and projective over A and*

$$\mathrm{rank}_A(P \otimes_A P') = \mathrm{rank}_A(P) \cdot \mathrm{rank}_A(P')$$

as functions on $\mathrm{Spec}(A)$ *(i.e. for any* $\mathfrak{p} \in \mathrm{Spec}(A)$ *we have that* $\mathrm{rank}_A(P \otimes_A P')(\mathfrak{p}) = \mathrm{rank}_A(P)(\mathfrak{p}) \cdot \mathrm{rank}_A(P')(\mathfrak{p})$*).*

Proof. We have that $P \otimes_A P'$ is projective by lemma 2.1.39. Moreover, if $(v_1, \dots, v_n)$ generates P and $(w_1, \dots, w_m)$ generates P', then $P \otimes_A P'$ is generated by $(v_i \otimes w_j)_{i=1,\dots,n,\, j=1,\dots,m}$. So $P \otimes_A P'$ is finitely generated over A.
Let now $\mathfrak{p} \in \mathrm{Spec}(A)$. By corollary 2.1.33(1), $P_{\mathfrak{p}}$ and $P'_{\mathfrak{p}}$ are both free of finite rank over $A_{\mathfrak{p}}$. Let $n := \mathrm{rank}_{A_{\mathfrak{p}}}(P_{\mathfrak{p}})$ and $m := \mathrm{rank}_{A_{\mathfrak{p}}}(P'_{\mathfrak{p}})$ (by definition of $\mathrm{rank}_A(P)$, this means that $n = \mathrm{rank}_A(P)(\mathfrak{p})$ and $m = \mathrm{rank}_A(P')(\mathfrak{p})$). Then $P_{\mathfrak{p}} \cong A_{\mathfrak{p}}^n$ and $P'_{\mathfrak{p}} \cong A_{\mathfrak{p}}^m$. Since the localization commutes with tensor products and direct sums (see lemmas 2.1.38 and 2.1.19, recalling that localization at $\mathfrak{p}$ corresponds to tensor product with $A_{\mathfrak{p}}$), we have that

$$(P \otimes_A P')_{\mathfrak{p}} \cong P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} P'_{\mathfrak{p}} \cong A_{\mathfrak{p}}^n \otimes_{A_{\mathfrak{p}}} A_{\mathfrak{p}}^m \cong \bigoplus_{\substack{i=1,\dots,n \\ j=1,\dots,m}} (A_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} A_{\mathfrak{p}}) \cong \bigoplus_{\substack{i=1,\dots,n \\ j=1,\dots,m}} A_{\mathfrak{p}} \cong A_{\mathfrak{p}}^{nm}$$

as $A_{\mathfrak{p}}$-modules (notice that lemma 2.1.19 gives only an isomorphism of A-modules, but it is immediate to check that in this case that isomorphism is also $A_{\mathfrak{p}}$-linear). Then, by definition of the rank for finitely generated projective A-modules, we get that

$$\mathrm{rank}_A(P \otimes_A P')(\mathfrak{p}) = nm = \mathrm{rank}_A(P)(\mathfrak{p}) \cdot \mathrm{rank}_A(P')(\mathfrak{p}) \ .$$

□

We will see now the link between faithfully projective and faithfully flat A-modules.

Lemma 2.1.41. *Let $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ be a sequence of A-modules. We have $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ is exact if and only if for every prime ideal $\mathfrak{p}$ of A the sequence of $A_{\mathfrak{p}}$-modules $(M_0)_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} (M_1)_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} (M_2)_{\mathfrak{p}}$ is exact.*

Proof. Notice that, as in the proof of lemma 2.1.28(2), we have $\mathrm{Ker}(g_{\mathfrak{p}}) = \mathrm{Ker}(g)_{\mathfrak{p}}$ and $\mathrm{Im}(f_{\mathfrak{p}}) = \mathrm{Im}(f)_{\mathfrak{p}}$, for every prime ideal $\mathfrak{p}$ of A.
Assume now that $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ is exact, i.e. $\mathrm{Ker}(g) = \mathrm{Im}(f)$. Then, for any prime ideal $\mathfrak{p}$ of A, we have that

$$\mathrm{Ker}(g_{\mathfrak{p}}) = \mathrm{Ker}(g)_{\mathfrak{p}} = \mathrm{Im}(f)_{\mathfrak{p}} = \mathrm{Im}(f_{\mathfrak{p}}) \ ,$$

which means that the sequence $(M_0)_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} (M_1)_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} (M_2)_{\mathfrak{p}}$ is exact.
Conversely, assume that, for every prime ideal $\mathfrak{p}$ of A, the sequence $(M_0)_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} (M_1)_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} (M_2)_{\mathfrak{p}}$ is exact, i.e. $\mathrm{Ker}(g_{\mathfrak{p}}) = \mathrm{Im}(f_{\mathfrak{p}})$. In particular, we have that $0 = g_{\mathfrak{p}} \circ f_{\mathfrak{p}} = (g \circ f)_{\mathfrak{p}}$ and so $0 = \mathrm{Im}((g \circ f)_{\mathfrak{p}}) = \mathrm{Im}(g \circ f)_{\mathfrak{p}}$ (the last equality

can be checked as in the proof of lemma 2.1.28(2)), for every prime ideal $\mathfrak{p}$ of A. By lemma 2.1.28(1), this implies that $\operatorname{Im}(g \circ f) = 0$, i.e. $g \circ f = 0$. It follows that $\operatorname{Im}(f) \subseteq \operatorname{Ker}(g)$. Consider now the quotient $\operatorname{Ker}(g)/\operatorname{Im}(f)$. Since the localization commutes with quotients, we have that

$$(\operatorname{Ker}(g)/\operatorname{Im}(f))_{\mathfrak{p}} \cong \operatorname{Ker}(g)_{\mathfrak{p}}/\operatorname{Im}(f)_{\mathfrak{p}} = \operatorname{Ker}(g_{\mathfrak{p}})/\operatorname{Im}(f_{\mathfrak{p}}) = 0$$

for any prime ideal $\mathfrak{p}$ of A. By lemma 2.1.28(1), we have $\operatorname{Ker}(g)/\operatorname{Im}(f) = 0$, i.e. $\operatorname{Ker}(g) = \operatorname{Im}(f)$. Hence $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ is exact. □

Lemma 2.1.42. *Let P be a finitely generated projective A-module. The following are equivalent:*

(i) P is faithfully flat;

(ii) for any A-module M, we have that $M = 0$ if and only if $M \otimes_A P = 0$;

(iii) the map $\mu : A \to \operatorname{End}_{\mathbb{Z}}(P)$, $a \mapsto (x \mapsto ax)$ is injective;

(iv) P is faithfully projective.

Proof. (i) $\Longrightarrow$ (ii) Let M be an A-module. Consider the sequence $0 \to M \to 0$ (with the only possible maps, i.e. the zero maps). Since P is faithfully flat, we have that $0 \to M \to 0$ is exact if and only if $0 = 0 \otimes_A P \to M \otimes_A P \to 0 \otimes_A P = 0$ is exact. On the other hand, by definition of exact sequence, we have that $0 \to M \to 0$ is exact if and only if $M = 0$ and $0 \to M \otimes_A P \to 0$ is exact if and only if $M \otimes_A P = 0$. Hence $M = 0$ if and only if $M \otimes_A P = 0$.

(ii) $\Longrightarrow$ (iii) First of all, notice that $\operatorname{End}_{\mathbb{Z}}(P)$ is an abelian group, with operation given by $(f+g)(x) = f(x)+g(x)$, for any $f, g \in \operatorname{End}_{\mathbb{Z}}(P)$, $x \in P$ (and identity element the zero map). We check now that $\mu : A \to \operatorname{End}_{\mathbb{Z}}(P)$ is well defined. Let $a \in A$. By definition of A-module, we have that $\mu(a)(x_1 + x_2) = a(x_1 + x_2) = ax_1 + ax_2 = \mu(a)(x_1) + \mu(a)(x_2)$ for any $x_1, x_2 \in P$. So $\mu(a) : P \to P$ is a group homomorphism, i.e. it is $\mathbb{Z}$-linear. Then $\mu(a) \in \operatorname{End}_{\mathbb{Z}}(P)$ for any $a \in A$, which shows that μ is well defined. Let now $a_1, a_2 \in A$. By definition of A-module, we have that

$$\begin{aligned}\mu(a_1 + a_2)(x) = (a_1 + a_2)x = a_1x + a_2x = \\ = \mu(a_1)(x) + \mu(a_2)(x) = (\mu(a_1) + \mu(a_2))(x)\end{aligned}$$

for any $x \in P$ and so $\mu(a_1 + a_2) = \mu(a_1) + \mu(a_2)$. Then μ is a group homomorphism from $(A, +)$ to $\operatorname{End}_{\mathbb{Z}}(P)$. So, in order to prove that μ is injective, it is enough to show that $\operatorname{Ker}(\mu) = 0$. We have that

$$\begin{aligned}\operatorname{Ker}(\mu) = \{a \in A \mid \mu(a) = 0\} = \\ = \{a \in A \mid \forall x \in P \quad 0 = \mu(a)(x) = ax\} = \operatorname{Ann}_A(P) \ .\end{aligned}$$

We know that $\operatorname{Ann}_A(P)$ is an ideal of A, so we can see it as an A-module. For any $a \in \operatorname{Ann}_A(P)$, $x \in P$ we have that $a \otimes x = (a \cdot 1) \otimes x = a(1 \otimes x) = 1 \otimes (ax) =$

$1 \otimes 0 = 0$. Then, since $\mathrm{Ann}_A(P) \otimes_A P$ is generated by pure tensors, we have that $\mathrm{Ann}_A(P) \otimes_A P = 0$. By assumption, this implies that $\mathrm{Ker}(\mu) = \mathrm{Ann}_A(P) = 0$. So μ is injective.

(iii) $\Longrightarrow$ (iv) Since we already know that P is finitely generated and projective, it is enough to check that $\mathrm{rank}_A(P) \geq 1$. Let $\mathfrak{p}$ be a prime ideal of A. Assume by contradiction that $P_\mathfrak{p} = 0$. Let $(w_1, \dots, w_n)$ be a set of generators of P. Since $P_\mathfrak{p} = 0$, for any $i = 1, \dots, n$ we have that $\frac{w_i}{1} = 0$, which means that there exists $u_i \in A \backslash \mathfrak{p}$ such that $u_i w_i = 0$. Define $u := \prod_{i=1}^n u_i$. Since $\mathfrak{p}$ is prime, we have that $A \backslash \mathfrak{p}$ is multiplicative and so $u \in A \backslash \mathfrak{p}$. For any $j = 1, \dots, n$, we have

$$uw_j = \left(\prod_{i=1}^n u_i \right) w_j = \left(\prod_{i \neq j} u_i \right) u_j w_j = \left(\prod_{i \neq j} u_i \right) \cdot 0 = 0 \, .$$

Since $(w_1, \dots, w_n)$ generates P and multiplication by u is A-linear, it follows that $ux = 0$ for any $x \in P$. This means that $\mu(u) = 0 = \mu(0)$. By assumptions, we must have that $u = 0 \in \mathfrak{p}$, which is a contradiction with the fact that $u \in A \backslash \mathfrak{p}$. Then $P_\mathfrak{p} \neq 0$, which implies that $\mathrm{rank}_{A_\mathfrak{p}}(P_\mathfrak{p}) \neq 0$ and, since the rank is a non-negative integer by definition, $\mathrm{rank}_A(P)(\mathfrak{p}) = \mathrm{rank}_{A_\mathfrak{p}}(P_\mathfrak{p}) \geq 1$.

(iv) $\Longrightarrow$ (i) Let $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ be a sequence of A-modules. Since P is projective, by corollary 2.1.22 we have that P is flat. Then, if $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ is exact, we have that also the induced sequence $M_0 \otimes_A P \xrightarrow{f \otimes \mathrm{id}_P} M_1 \otimes_A P \xrightarrow{g \otimes \mathrm{id}_P} M_2 \otimes_A P$ is exact.
Conversely, assume that $M_0 \otimes_A P \xrightarrow{f \otimes \mathrm{id}_P} M_1 \otimes_A P \xrightarrow{g \otimes \mathrm{id}_P} M_2 \otimes_A P$ is exact. Let $\mathfrak{p}$ be a prime ideal of A. By lemma 2.1.41, we have that the sequence of $A_\mathfrak{p}$-modules

$$(M_0 \otimes_A P)_\mathfrak{p} \xrightarrow{(f \otimes \mathrm{id}_P)_\mathfrak{p}} (M_1 \otimes_A P)_\mathfrak{p} \xrightarrow{(g \otimes \mathrm{id}_P)_\mathfrak{p}} (M_2 \otimes_A P)_\mathfrak{p}$$

is exact. By lemma 2.1.38, we have that $(M_i \otimes_A P_i)_\mathfrak{p} \cong (M_i)_\mathfrak{p} \otimes_{A_\mathfrak{p}} P_\mathfrak{p}$ as $A_\mathfrak{p}$-modules, for $i = 0, 1, 2$. Denote by $\Phi_i : (M_i)_\mathfrak{p} \otimes_{A_\mathfrak{p}} P_\mathfrak{p} \to (M_i \otimes_A P)_\mathfrak{p}$ the corresponding isomorphism, as in the proof of that lemma, i.e. $\Phi_i \left(\frac{m}{s} \otimes \frac{x}{t} \right) = \frac{m \otimes x}{st}$ for any $m \in M_i$, $x \in P$, $s, t \in A \backslash \mathfrak{p}$. Consider the following diagram.

$$\begin{array}{ccccc}
(M_0)_\mathfrak{p} \otimes_{A_\mathfrak{p}} P_\mathfrak{p} & \xrightarrow{f_\mathfrak{p} \otimes \mathrm{id}_{P_\mathfrak{p}}} & (M_1)_\mathfrak{p} \otimes_{A_\mathfrak{p}} P_\mathfrak{p} & \xrightarrow{g_\mathfrak{p} \otimes \mathrm{id}_{P_\mathfrak{p}}} & (M_2)_\mathfrak{p} \otimes_{A_\mathfrak{p}} P_\mathfrak{p} \\
\downarrow \Phi_0 & & \downarrow \Phi_1 & & \downarrow \Phi_2 \\
(M_0 \otimes_A P)_\mathfrak{p} & \xrightarrow{(f \otimes \mathrm{id}_P)_\mathfrak{p}} & (M_1 \otimes_A P)_\mathfrak{p} & \xrightarrow{(g \otimes \mathrm{id}_P)_\mathfrak{p}} & (M_2 \otimes_A P)_\mathfrak{p}
\end{array}$$

For any $m \in M_0$, $x \in P$, $s, t \in A \backslash \mathfrak{p}$, we have that

$$\begin{aligned}
(\Phi_1 \circ (f_\mathfrak{p} \otimes \mathrm{id}_{P_\mathfrak{p}})) \left(\frac{m}{s} \otimes \frac{x}{t} \right) &= \Phi_1 \left(f_\mathfrak{p} \left(\frac{m}{s} \right) \otimes \frac{x}{t} \right) = \\
&= \Phi_1 \left(\frac{f(m)}{s} \otimes \frac{x}{t} \right) = \frac{f(m) \otimes x}{st} = \frac{(f \otimes \mathrm{id}_P)(m \otimes x)}{st} = \\
&= (f \otimes \mathrm{id}_P)_\mathfrak{p} \left(\frac{m \otimes x}{st} \right) = (f \otimes \mathrm{id}_P)_\mathfrak{p} \left(\Phi_0 \left(\frac{m}{s} \otimes \frac{x}{t} \right) \right) \, .
\end{aligned}$$

So $\Phi_1 \circ (f_\mathfrak{p} \otimes \mathrm{id}_{P_\mathfrak{p}}) = (f \otimes \mathrm{id}_P)_\mathfrak{p} \circ \Phi_0$ (since the maps are $A_\mathfrak{p}$-linear, it is enough to check equality on pure tensors). Analogously, one can check that $\Phi_2 \circ (g_\mathfrak{p} \otimes \mathrm{id}_{P_\mathfrak{p}}) = (g \otimes \mathrm{id}_P)_\mathfrak{p} \circ \Phi_1$. So the diagram is commutative. Since the lower row is exact, the upper one is also exact. Since P is finitely generated and projective, by corollary 2.1.33 we have that $P_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module of finite rank. Then $P_\mathfrak{p} \cong A_\mathfrak{p}^n$ as $A_\mathfrak{p}$-modules, where $n = \mathrm{rank}_{A_\mathfrak{p}}(P_\mathfrak{p})$. If $\vartheta : P_\mathfrak{p} \to A_\mathfrak{p}^n$ is an isomorphism of $A_\mathfrak{p}$-modules, we have induced isomorphisms of $A_\mathfrak{p}$-modules $\mathrm{id}_{M_i} \otimes \vartheta : (M_i)_\mathfrak{p} \otimes_{A_\mathfrak{p}} P_\mathfrak{p} \to (M_i)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}^n$, for $i = 0, 1, 2$. Moreover, $(\mathrm{id}_{M_1} \otimes \vartheta) \circ (f_\mathfrak{p} \otimes \mathrm{id}_{P_\mathfrak{p}}) = f_\mathfrak{p} \otimes \vartheta = (f_\mathfrak{p} \otimes \mathrm{id}_{A_\mathfrak{p}^n}) \circ (\mathrm{id}_{M_0} \otimes \vartheta)$ and $(\mathrm{id}_{M_2} \otimes \vartheta) \circ (g_\mathfrak{p} \otimes \mathrm{id}_{P_\mathfrak{p}}) = g_\mathfrak{p} \otimes \vartheta = (g_\mathfrak{p} \otimes \mathrm{id}_{A_\mathfrak{p}^n}) \circ (\mathrm{id}_{M_1} \otimes \vartheta)$. So the following diagram is commutative.

$$\begin{array}{ccccc}
(M_0)_\mathfrak{p} \otimes_{A_\mathfrak{p}} P_\mathfrak{p} & \xrightarrow{f_\mathfrak{p} \otimes \mathrm{id}_{P_\mathfrak{p}}} & (M_1)_\mathfrak{p} \otimes_{A_\mathfrak{p}} P_\mathfrak{p} & \xrightarrow{g_\mathfrak{p} \otimes \mathrm{id}_{P_\mathfrak{p}}} & (M_2)_\mathfrak{p} \otimes_{A_\mathfrak{p}} P_\mathfrak{p} \\
\downarrow {\scriptstyle \mathrm{id}_{M_0} \otimes \vartheta} & & \downarrow {\scriptstyle \mathrm{id}_{M_1} \otimes \vartheta} & & \downarrow {\scriptstyle \mathrm{id}_{M_2} \otimes \vartheta} \\
(M_0)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}^n & \xrightarrow{f_\mathfrak{p} \otimes \mathrm{id}_{A_\mathfrak{p}^n}} & (M_1)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}^n & \xrightarrow{g_\mathfrak{p} \otimes \mathrm{id}_{A_\mathfrak{p}^n}} & (M_2)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}^n
\end{array}$$

Then, since the upper row is exact, the lower row is also exact. By lemma 2.1.19 (with $A_\mathfrak{p}$ instead of A and exchanging the order of the factors), we have isomorphisms of $A_\mathfrak{p}$-modules $\psi_{(M_i)_\mathfrak{p}} : (M_i)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}^n \to ((M_i)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p})^n$, for $i = 0, 1, 2$. On the other hand, we have canonical isomorphisms of $A_\mathfrak{p}$-modules $\sigma_i : (M_i)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p} \to (M_i)_\mathfrak{p}$, $m \otimes \lambda \mapsto \lambda m$, for $i = 0, 1, 2$. Consider the following diagram.

$$\begin{array}{ccccc}
(M_0)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}^n & \xrightarrow{f_\mathfrak{p} \otimes \mathrm{id}_{A_\mathfrak{p}^n}} & (M_1)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}^n & \xrightarrow{g_\mathfrak{p} \otimes \mathrm{id}_{A_\mathfrak{p}^n}} & (M_2)_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}^n \\
\downarrow {\scriptstyle \sigma_0^n \circ \psi_{(M_0)_\mathfrak{p}}} & & \downarrow {\scriptstyle \sigma_1^n \circ \psi_{(M_1)_\mathfrak{p}}} & & \downarrow {\scriptstyle \sigma_2^n \circ \psi_{(M_2)_\mathfrak{p}}} \\
(M_0)_\mathfrak{p}^n & \xrightarrow{f_\mathfrak{p}^n} & (M_1)_\mathfrak{p}^n & \xrightarrow{g_\mathfrak{p}^n} & (M_2)_\mathfrak{p}^n
\end{array}$$

For any $m \in M_0$, $(\lambda_1, \ldots, \lambda_n) \in A_\mathfrak{p}^n$ we have that

$$\begin{aligned}
&(\sigma_1^n \circ \psi_{(M_1)_\mathfrak{p}} \circ (f_\mathfrak{p} \otimes \mathrm{id}_{A_\mathfrak{p}^n}))(m \otimes (\lambda_1, \ldots, \lambda_n)) = \\
&= \sigma_1^n(\psi_{(M_1)_\mathfrak{p}}(f_\mathfrak{p}(m) \otimes (\lambda_1, \ldots, \lambda_n))) = \sigma_1^n((f_\mathfrak{p}(m) \otimes \lambda_1, \ldots, f_\mathfrak{p}(m) \otimes \lambda_n)) = \\
&= (\sigma_1(f_\mathfrak{p}(m) \otimes \lambda_1), \ldots, \sigma_1(f_\mathfrak{p}(m) \otimes \lambda_n)) = (\lambda_1 f_\mathfrak{p}(m), \ldots, \lambda_n f_\mathfrak{p}(m)) = \\
&= (f_\mathfrak{p}(\lambda_1 m), \ldots, f_\mathfrak{p}(\lambda_n m)) = f_\mathfrak{p}^n((\lambda_1 m, \ldots, \lambda_n m)) = \\
&= f_\mathfrak{p}((\sigma_0(m \otimes \lambda_1), \ldots, \sigma_0(m \otimes \lambda_n))) = f_\mathfrak{p}(\sigma_0^n((m \otimes \lambda_1, \ldots, m \otimes \lambda_n))) = \\
&= (f_\mathfrak{p} \circ \sigma_0^n)(\psi_{(M_0)_\mathfrak{p}}(m \otimes (\lambda_1, \ldots, \lambda_n))) .
\end{aligned}$$

So $\sigma_1^n \circ \psi_{(M_1)_\mathfrak{p}} \circ (f_\mathfrak{p} \otimes \mathrm{id}_{A_\mathfrak{p}^n}) = f_\mathfrak{p} \circ \sigma_0^n \circ \psi_{(M_0)_\mathfrak{p}}$ (since the maps are $A_\mathfrak{p}$-linear, it is enough to check equality on pure tensors). Analogously, one can show that $\sigma_2^n \circ \psi_{(M_2)_\mathfrak{p}} \circ (g_\mathfrak{p} \otimes \mathrm{id}_{A_\mathfrak{p}^n}) = g_\mathfrak{p} \circ \sigma_1^n \circ \psi_{(M_1)_\mathfrak{p}}$. So the diagram is commutative. Since the upper row is exact, the lower row must also be exact. This means that $\mathrm{Ker}(g_\mathfrak{p}^n) = \mathrm{Im}(f_\mathfrak{p}^n)$. It is easy to check that

$$\mathrm{Ker}(g_\mathfrak{p}^n) = \mathrm{Ker}(g_\mathfrak{p})^n$$

and

$$\mathrm{Im}(f_\mathfrak{p}^n) = \mathrm{Im}(f_\mathfrak{p})^n$$

(see the proof of corollary 2.1.20). Then we must have $\mathrm{Ker}(g_{\mathfrak{p}}) = \mathrm{Im}(f_{\mathfrak{p}})$, i.e. the sequence $(M_0)_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} (M_1)_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} (M_2)_{\mathfrak{p}}$ is exact. Since this holds for any prime ideal $\mathfrak{p}$ of A, applying again lemma 2.1.41 we get that $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ is exact. Hence P is faithfully flat.

□

Now we want to define the trace also for endomorphisms of a finitely generated projective A-module (see 2.1.1 for the definition in the case of free A-modules of finite rank). This will later allow us to define projective separable A-algebras. For any A-module P, we denote by P^* the *dual* of P, i.e. $P^* := \mathrm{Hom}_A(A, P)$.

Lemma 2.1.43. *Let M be an A-module. For any A-module P we have an A-linear map*

$$\vartheta_{P,M} : P^* \otimes_A M \to \mathrm{Hom}_A(P, M),\ f \otimes m \mapsto (p \mapsto f(p) \cdot m)$$

(extended by linearity). If $P = \oplus_{i=1}^n P_i$, for some A-modules $P_1, \dots, P_n$, then $\vartheta_{P,M}$ is bijective if and only if $\vartheta_{P_i,M}$ is bijective for every $i = 1, \dots, n$.

Proof. First of all, we prove that $\vartheta_{P,M}$ is well defined, for any A-module P. For any $f \in P^*$, $m \in M$, consider the map $\vartheta_{f,m} : P \to M,\ p \mapsto f(p) \cdot m$. For any $\lambda_1, \lambda_2 \in A$, $p_1, p_2 \in P$, we have that $f(\lambda_1 p_1 + \lambda_2 p_2) = \lambda_1 f(p_1) + \lambda_2 f(p_2)$, because f is A-linear. So

$$\begin{aligned}\vartheta_{f,m}(\lambda_1 p_1 + \lambda_2 p_2) &= f(\lambda_1 p_1 + \lambda_2 p_2) \cdot m = (\lambda_1 f(p_1) + \lambda_2 f(p_2)) \cdot m = \\ &= \lambda_1 (f(p_1) \cdot m) + \lambda_2 (f(p_2) \cdot m) = \lambda_1 \vartheta_{f,m}(p_1) + \lambda_2 \vartheta_{f,m}(p_2)\ .\end{aligned}$$

Then $\vartheta_{f,m}$ is A-linear, i.e. $\vartheta_{f,m} \in \mathrm{Hom}_A(P, M)$. So we can consider the map

$$\Theta_{P,M} : P^* \times M \to \mathrm{Hom}_A(P, M),\ f \mapsto \vartheta_{f,m}\ .$$

We claim that this map is A-bilinear. Let $\lambda_1, \lambda_2 \in A$, $f_1, f_2 \in P^*$ and $m \in M$. For any $p \in P$, we have that $(\lambda_1 f_1 + \lambda_2 f_2)(p) = \lambda_1 f_1(p) + \lambda_2 f_2(p)$, by definition of the A-module structure on P^*, and so

$$\begin{aligned}\vartheta_{\lambda_1 f_1 + \lambda_2 f_2, m}(p) &= (\lambda_1 f_1 + \lambda_2 f_2)(p) \cdot m = (\lambda_1 f_1(p) + \lambda_2 f_2(p)) \cdot m = \\ &= \lambda_1 (f_1(p) \cdot m) + \lambda_2 (f_2(p) \cdot m) = \lambda_1 \vartheta_{f_1,m}(p) + \lambda_2 \vartheta_{f_2,m}(p)\ .\end{aligned}$$

Then

$$\begin{aligned}\Theta_{P,M}((\lambda_1 f_1 + \lambda_2 f_2, m)) &= \vartheta_{\lambda_1 f_1 + \lambda_2 f_2, m} = \\ &= \lambda_1 \vartheta_{f_1,m} + \lambda_2 \vartheta_{f_2,m} = \lambda_1 \Theta_{P,M}((f_1, m)) + \lambda_2 \Theta_{P,M}((f_2, m))\ .\end{aligned}$$

On the other hand, if $f \in P^*$, $\lambda_1, \lambda_2 \in A$ and $m_1, m_2 \in M$, then for any $p \in P$ we have

$$\begin{aligned}\vartheta_{f, \lambda_1 m_1 + \lambda_2 m_2}(p) &= f(p) \cdot (\lambda_1 m_1 + \lambda_2 m_2) = \\ &= \lambda_1 (f(p) \cdot m_1) + \lambda_2 (f(p) \cdot m_2) = \lambda_1 \vartheta_{f,m_1}(p) + \lambda_2 \vartheta_{f,m_2}(p)\ .\end{aligned}$$

So

$$\begin{aligned}\Theta_{P,M}((f, \lambda_1 m_1 + \lambda_2 m_2)) &= \vartheta_{f,\lambda_1 m_1 + \lambda_2 m_2} = \\ &= \lambda_1 \vartheta_{f,m_1} + \lambda_2 \vartheta_{f,m_2} = \lambda_1 \Theta_{P,M}((f, m_1)) + \lambda_2 \Theta_{P,M}((f, m_2)) \ .\end{aligned}$$

This proves that $\Theta_{P,M}$ is A-bilinear, so it induces an A-linear map $\vartheta_{P,M} : P^* \otimes_A M \to \mathrm{Hom}_A(P, M)$ as in the statement.
Assume now that $P = \bigoplus_{i=1}^n P_i$. As in lemma 2.1.9, consider the isomorphisms of A-modules $\varphi_M : \mathrm{Hom}_A(P, M) \to \prod_{i=1}^n \mathrm{Hom}_A(P_i, M)$ and $\varphi_A : P^* = \mathrm{Hom}_A(P, A) \to \prod_{i=1}^n \mathrm{Hom}_A(P_i, A) = \prod_{i=1}^n (P_i)^*$. Since the direct sum of a *finite* family of A-modules coincides with its direct product, we have $\prod_{i=1}^n \mathrm{Hom}_A(P_i, M) = \bigoplus_{i=1}^n \mathrm{Hom}_A(P_i, M)$ and $\prod_{i=1}^n (P_i)^* = \bigoplus_{i=1}^n (P_i)^*$. Since φ_A is an isomorphism, also $\varphi_A \otimes \mathrm{id}_M : P^* \otimes_A M \to (\bigoplus_{i=1}^n P_i^*) \otimes_A M$ is an isomorphism. Consider moreover the isomorphism $\psi_M : (\bigoplus_{i=1}^n P_i^*) \otimes_A M \to \bigoplus_{i=1}^n (P_i^* \otimes_A M)$ as in lemma 2.1.19. Then we have the following diagram.

$$\begin{array}{ccc} P^* \otimes_A M & \xrightarrow{\ \vartheta_{P,M}\ } & \mathrm{Hom}_A(P, M) \\ {\scriptstyle \psi_M \circ (\varphi_A \otimes \mathrm{id}_M)} \downarrow & & \downarrow {\scriptstyle \varphi_M} \\ \bigoplus_{i=1}^n (P_i^* \otimes_A M) & \xrightarrow{\ \bigoplus_{i=1}^n \vartheta_{P_i,M}\ } & \bigoplus_{i=1}^n \mathrm{Hom}_A(P_i, M) \end{array}$$

We claim that this diagram is commutative. Let $f \in P^*$ and $m \in M$. We have that

$$\varphi_M(\vartheta_{P,M}(f \otimes m)) = \varphi_M(\vartheta_{f,m}) = (\vartheta_{f,m} \circ q_i)_{i=1,\ldots,n} \ ,$$

where we defined $q_j : P_j \to P,\ x \mapsto (\delta_{ij} x)_{i=1,\ldots,n}$ for any $j = 1, \ldots, n$. On the other hand,

$$\begin{aligned}&\left(\bigoplus_{i=1}^n \vartheta_{P_i,M}\right) ((\psi_M \circ (\varphi_A \otimes \mathrm{id}_M))(f \otimes m)) = \\ &= \left(\bigoplus_{i=1}^n \vartheta_{P_i,M}\right) (\psi_M(\varphi_A(f) \otimes m)) = \left(\bigoplus_{i=1}^n \vartheta_{P_i,M}\right) (\psi_M((f \circ q_i)_{i=1,\ldots,n} \otimes m)) = \\ &= \left(\bigoplus_{i=1}^n \vartheta_{P_i,M}\right) (((f \circ q_i) \otimes m)_{i=1,\ldots,n}) = (\vartheta_{f \circ q_i, m})_{i=1,\ldots,n} \ .\end{aligned}$$

For any $i = 1, \ldots, n$, we have that

$$(\vartheta_{f,m} \circ q_i)(p) = \vartheta_{f,m}(q_i(p)) = f(q_i(p)) \cdot m = (f \circ q_i)(p) \cdot m = \vartheta_{f \circ q_i, m}(p)$$

for any $p \in P_i$ and so $\vartheta_{f,m} \circ q_i = \vartheta_{f \circ q_i, m}$. This proves that

$$(\varphi_M \circ \vartheta_{P,M})(f \otimes m) = \left(\left(\bigoplus_{i=1}^n \vartheta_{P_i,M}\right) \circ (\psi_M \circ (\varphi_A \otimes \mathrm{id}_M))\right)(f \otimes m) \ .$$

Then $\varphi_M \circ \vartheta_{P,M} = (\bigoplus_{i=1}^n \vartheta_{P_i,M}) \circ (\psi_M \circ (\varphi_A \otimes \mathrm{id}_M))$ (since we are dealing with A-linear maps, it is enough to check equality on pure tensors), i.e. the diagram is commutative. Since φ_M and $\psi_M \circ (\varphi_A \otimes \mathrm{id}_M)$ are isomorphisms, it follows that $\vartheta_{P,M}$ is bijective if and only if $\bigoplus_{i=1}^n \vartheta_{P_i,M}$ is bijective. It is easy to prove that

$$\mathrm{Ker}\left(\bigoplus_{i=1}^n \vartheta_{P_i,M}\right) = \bigoplus_{i=1}^n \mathrm{Ker}(\vartheta_{P_i,M})$$

and

$$\mathrm{Im}\left(\bigoplus_{i=1}^n \vartheta_{P_i,M}\right) = \bigoplus_{i=1}^n \mathrm{Im}(\vartheta_{P_i,M})$$

(see the proof of corollary 2.1.20). So we have that $\mathrm{Ker}\left(\bigoplus_{i=1}^n \vartheta_{P_i,M}\right) = 0$ if and only if $\mathrm{Ker}(\vartheta_{P_i,M}) = 0$ for any $i = 1, \ldots, n$, i.e. $\bigoplus_{i=1}^n \vartheta_{P_i,M}$ is injective if and only if $\vartheta_{P_i,M}$ is injective for any $i = 1, \ldots, n$, and $\mathrm{Im}\left(\bigoplus_{i=1}^n \vartheta_{P_i,M}\right) = \bigoplus_{i=1}^n \mathrm{Hom}_A(P_i, M)$ if and only if $\mathrm{Im}(\vartheta_{P_i,M}) = \mathrm{Hom}_A(P_i, M)$ for any $i = 1, \ldots, n$, i.e. $\bigoplus_{i=1}^n \vartheta_{P_i,M}$ is surjective if and only if $\vartheta_{P_i,M}$ is surjective for any $i = 1, \ldots, n$. Hence $\bigoplus_{i=1}^n \vartheta_{P_i,M}$ is bijective if and only if $\vartheta_{P_i,M}$ is bijective for every $i = 1, \ldots, n$, which ends the proof. □

Remark 2.1.44. A key point in the proof of lemma 2.1.43 was the fact that we were dealing with a *finite* direct sum. The result is not true for infinite direct sums. Otherwise the corollary we are about to prove would hold for any projective A-module and, in the case when $A = k$ is a field, this would imply that $\vartheta_{P,M}$ is bijective for every two k-vector spaces P and M (because all k-vector spaces are free and hence projective). A counterexample is given by $P = M = k[x]$.

Corollary 2.1.45. *Let P and M be A-modules, with P finitely generated and projective. The map $\vartheta_{P,M} : P^* \otimes_A M \to \mathrm{Hom}_A(P, M)$ defined in lemma 2.1.43 is an isomorphism of A-modules.*

Proof. We already know that $\vartheta_{P,M}$ is A-linear, so we have to prove only that it is bijective. Since P is finitely generated and projective, by corollary 2.1.15 there exist an A-module Q and an $n \in \mathbb{N}$ such that $P \oplus Q \cong A^n$. By lemma 2.1.43, in order to prove that $\vartheta_{P,M}$ is bijective, it is enough to show that $\vartheta_{A^n,M}$ is bijective. By the same lemma, in order to prove that $\vartheta_{A^n,M}$ is bijective, it is enough to prove that $\vartheta_{A,M}$ is bijective. We have that $A^* \cong A$ via $\varphi : A^* \to A,\ f \mapsto f(1)$. Then $\varphi \otimes \mathrm{id}_M : A^* \otimes_A M \to A \otimes_A M$ is also an isomorphism. Moreover, $A \otimes_A M \cong M$ via $\psi : A \otimes_A M \to M,\ a \otimes m \to am$ and $\mathrm{Hom}_A(A, M) \cong M$ via $\varphi' : \mathrm{Hom}_A(A, M) \to M,\ f \mapsto f(1)$. Consider now the following diagram.

$$\begin{array}{ccc} A^* \otimes_A M & \xrightarrow{\vartheta_{A,M}} & \mathrm{Hom}_A(A, M) \\ \psi \circ (\varphi \otimes \mathrm{id}_M) \Big\downarrow & & \Big\downarrow \varphi' \\ M & \xrightarrow{\mathrm{id}_M} & M \end{array}$$

For any $f \in A^*$, $m \in M$, we have that

$$\begin{aligned} \varphi'(\vartheta_{A,M}(f \otimes m)) = \varphi'(\vartheta_{f,m}) = \vartheta_{f,m}(1) = f(1) \cdot m = \\ = \varphi(f)m = \psi(\varphi(f) \otimes m) = \psi((\varphi \otimes \mathrm{id}_M)(f \otimes m)) \,. \end{aligned}$$

So $\varphi' \circ \vartheta_{A,M} = \psi \circ (\varphi \otimes \mathrm{id}_M)$ (by linearity, it is enough to check equality on pure tensors). Since φ', ψ and $\varphi \otimes \mathrm{id}_M$ are isomorphisms, we get that $\vartheta_{A,M} = (\varphi')^{-1} \circ \psi \circ (\varphi \otimes \mathrm{id}_M)$ is bijective, because it is a composition of bijections. This ends the proof. □

Lemma 2.1.46. *Let P be an A-module. For any $f \in P^*$, $p \in P$, define $\alpha_P(f \otimes p) = f(p)$. This definition can be extended to an A-linear map $\alpha_P : P^* \otimes_A P \to A$.*

Proof. By the universal property of the tensor product, it is enough to prove that the map $P^* \times P \to A$, $(f, p) \mapsto f(p)$ is A-bilinear. This is immediate: the linearity in f follows from the definition of the A-module structure on P^* and the linearity in p follows from the linearity of f. □

Definition 2.1.47. Let P be a finitely generated projective A-module, $\vartheta_{P,P} : P^* \otimes_A P \to \mathrm{Hom}_A(P, P)$ as in lemma 2.1.43 and $\alpha_P : P^* \otimes_A P \to A$ as in lemma 2.1.46. For any endomorphism $f \in \mathrm{End}_A(P) := \mathrm{Hom}_A(P, P)$, we define the *trace* of f over A as $\mathrm{Tr}(f) = (\alpha_P \circ \vartheta_{P,P}^{-1})(f)$ (we will write $\mathrm{Tr}_{P/A}(f)$ when confusion can arise).

Remark 2.1.48. The map $\mathrm{Tr} : \mathrm{End}_A(P) \to A$, $f \mapsto \mathrm{Tr}(f)$ is A-linear, because it is the composition of the A-linear maps $\vartheta_{P,P}$ and α_P.

The following lemma gives a more explicit description of the trace.

Lemma 2.1.49. *Let P be a finitely generated and projective A-module. Then:*

(1) there exist $n \in \mathbb{N}$, $x_1, \dots, x_n \in P$ and $f_1, \dots, f_n \in P^*$ such that, for every $x \in P$, we have $x = \sum_{i=1}^n f_i(x) x_i$;

(2) if $n \in \mathbb{N}$, $x_1, \dots, x_n \in P$ and $f_1, \dots, f_n \in P^*$ are as in point (1), then for every $\varphi \in \mathrm{End}_A(P)$ we have that $\mathrm{Tr}(\varphi) = \sum_{i=1}^n f_i(\varphi(x_i))$.

Proof. (1) Since P is finitely generated and projective, by corollary 2.1.15 there exists an A-module Q and an $n \in \mathbb{N}$ such that $P \oplus Q \cong A^n$. Then $P \oplus Q$ is free of rank n, which implies that it has a basis $(w_1, \dots, w_n)$. For any $i = 1, \dots, n$, define $w_i^* : P \oplus Q \to A$, $w_j \mapsto \delta_{ij}$, extended by linearity. Let $w \in P \oplus Q$. Then there exists a unique n-tuple $(a_1, \dots, a_n)$, with $a_i \in A$ for any $i = 1, \dots n$, such that $w = \sum_{i=1}^n a_i w_i$. For any $j = 1, \dots, n$ we have that

$$w_j^*(w) = w_j^* \left(\sum_{i=1}^n a_i w_i \right) = \sum_{i=1}^n a_i w_j^*(w_i) = \sum_{i=1}^n a_i \delta_{ij} = a_j \ .$$

So $w = \sum_{i=1}^n w_i^*(w) w_i$, for any $w \in P \oplus Q$. Define now $p_P : P \oplus Q \to P$, $(p, q) \mapsto p$ and $\iota_P : P \to P \oplus Q$, $p \mapsto (p, 0)$. Then p_P and ι_P are clearly A-linear and $p_P \circ \iota_P = \mathrm{id}_P$. For any $i = 1, \dots, n$ define $x_i := p_P(w_i) \in P$ and $f_i := w_i^* \circ \iota_P \in \mathrm{Hom}_A(P, A) = P^*$. For any $x \in P$ we have that

$$x = p_P(\iota_P(x)) = p_P \left(\sum_{i=1}^n w_i^*(\iota_P(x)) w_i \right) = \\ = \sum_{i=1}^n (w_i^* \circ \iota_P)(x) p_P(w_i) = \sum_{i=1}^n f_i(x) x_i \ ,$$

as we wanted.

(2) Let $\varphi \in \mathrm{End}_A(P) = \mathrm{Hom}_A(P,P)$. Then, for any $i = 1, \ldots, n$, we have that $f_i \circ \varphi \in \mathrm{Hom}_A(P,A) = P^*$. Consider $\sum_{i=1}^n (f_i \circ \varphi) \otimes x_i \in P^* \otimes P$. Applying the definition of $\vartheta_{P,P}$ (lemma 2.1.43), we get that

$$\vartheta_{P,P}\left(\sum_{i=1}^n (f_i \circ \varphi) \otimes x_i\right)(x) = \sum_{i=1}^n (f_i \circ \varphi)(x)x_i = \sum_{i=1}^n f_i(\varphi(x))x_i = \varphi(x)$$

for any $x \in P$. So $\vartheta_{P,P}\left(\sum_{i=1}^n (f_i \circ \varphi) \otimes x_i\right) = \varphi$, which implies that $\sum_{i=1}^n (f_i \circ \varphi) \otimes x_i = \vartheta_{P,P}^{-1}(\varphi)$. Then the definition 2.1.47 gives us

$$\begin{aligned}\mathrm{Tr}(\varphi) &= (\alpha_P \circ \vartheta_{P,P}^{-1})(\varphi) = \\ &= \alpha_P\left(\sum_{i=1}^n (f_i \circ \varphi) \otimes x_i\right) = \sum_{i=1}^n (f_i \circ \varphi)(x_i) = \sum_{i=1}^n f_i(\varphi(x_i)) \,.\end{aligned}$$

□

Remark 2.1.50. (1) What we did in point (1) of lemma 2.1.49 for $P \oplus Q$ can be done for any free A-module F of finite rank: if $(w_1, \ldots, w_n)$ is a basis of F (see remark 2.1.2), then for any $i = 1, \ldots, n$ we can define $w_i^* \in F^*$ by setting $w_i^*(w_j) = \delta_{ij}$ for every $j = 1, \ldots, n$ and extending linearly. Then we have $w = \sum_{i=1}^n w_i^*(w)w_i$ for any $w \in F$. It is easy to check that $(w_1^*, \ldots, w_n^*)$ is a basis of F^*, called the *dual basis* of $(w_1, \ldots, w_n)$. What lemma 2.1.49(1) says is that, even if in the case of an arbitrary projective A-module P we do not have a basis, we have a system of generators $(x_1, \ldots, x_n)$ of P and a "dual" system of generators $(f_1, \ldots, f_n)$ of P^* that behave in a similar way. Indeed, from the statement of 2.1.49(1) it is clear that $(x_1, \ldots, x_n)$ generates P and, on the other hand, for any $f \in P^*$ we have that $f = \sum_{i=1}^n f(x_i)f_i$, because $f(x) = f\left(\sum_{i=1}^n f_i(x)x_i\right) = \sum_{i=1}^n f_i(x)f(x_i)$ for any $x \in P$. However, while all bases of a free module of finite rank have the same cardinality (unless $A = 0$, see remark 2.1.2), the n that appears in the statement of lemma 2.1.49(1) is not unique. Indeed, in the proof n was the rank of the free A-module $P \oplus Q$, but if we choose a different Q we can get a different rank. For example, we can take $Q' = Q \oplus A$ and then $P \oplus Q' = P \oplus (Q \oplus A) \cong (P \oplus Q) \oplus A$ has rank $n+1$.

(2) Let $n, m \in \mathbb{N}$, $x_1, \ldots, x_n, y_1, \ldots, y_m \in P$ and $f_1, \ldots, f_n, g_1, \ldots, g_m \in P^*$ be such that $x = \sum_{i=1}^n f_i(x)x_i = \sum_{j=1}^m g_j(x)y_j$ for every $x \in P$. From lemma 2.1.49(2) it follows that, for every $\varphi \in \mathrm{End}_A(P)$,

$$\sum_{i=1}^n f_i(\varphi(x_i)) = \mathrm{Tr}(\varphi) = \sum_{j=1}^m g_j(\varphi(y_j)) \,.$$

This could be proved directly with some computations and then we could take the formula in 2.1.49(2) as the definition of the trace.

(3) We can use lemma 2.1.49 to prove that the two definitions of trace (2.1.1 and 2.1.47) coincide when P is a finitely generated and free A-module. Let P

be a free A-module with basis $(w_1, \dots, w_n)$ and let $(w_1^*, \dots, w_n^*)$ be the dual basis. As in point (1), we have that $w = \sum_{i=1}^n w_i^*(w)w_i$ for any $w \in P$. Let $\varphi \in \mathrm{End}_A(P)$. For any $i = 1, \dots, n$ we have that $\varphi(w_i) = \sum_{j=1}^n w_j^*(\varphi(w_i))w_j$, which means that $a_{ij} = w_j^*(\varphi(w_i))$ for any $j = 1, \dots, n$, where $a_{i1}, \dots, a_{in}$ are as in the definition 2.1.1. By lemma 2.1.49 we have that

$$\mathrm{Tr}_{\mathrm{projective}}(\varphi) = \sum_{i=1}^n w_i^*(\varphi(w_i)) = \sum_{i=1}^n a_{ii} = \mathrm{Tr}_{\mathrm{free}}(\varphi) ,$$

where we denoted by $\mathrm{Tr}_{\mathrm{projective}}$ the trace defined in 2.1.47 and by $\mathrm{Tr}_{\mathrm{free}}$ the trace defined in 2.1.1.

Now we turn our attention to A-algebras.

Definition 2.1.51. Let B be an A-algebra.

(1) We say that B is a *finite projective* A-algebra if it is finitely generated and projective as an A-module. In this case, we write $[B : A]$ for $\mathrm{rank}_A(B)$ (see the definition 2.1.35(1)).

(2) We say that B is *faithfully projective* if it is finitely generated and faithfully projective as an A-module, i.e. if it is a finite projective A-algebra with $[B : A] \geq 1$ (i.e. $[B : A](\mathfrak{p}) \geq 1$ for any $\mathfrak{p} \in \mathrm{Spec}(A)$).

(3) We say that B is a *(faithfully) flat* A-algebra if it is (faithfully) flat as an A-module.

We prove some easy properties about finite projective A-algebras, which we will need in the following section.

Lemma 2.1.52. *Let $B_1, \dots, B_n$ be A-algebras and define $B := \prod_{i=1}^n B_i$. Then B is a finite projective A-algebra if and only if B_i is a finite projective A-algebra for every $i = 1, \dots, n$.*

Proof. By definition of product of A-algebras, we have that, as an A-module, $B = \prod_{i=1}^n B_i$ coincides with the direct sum $\bigoplus_{i=1}^n B_i$.
Assume now that B_i is a finite projective A-algebra for every $i = 1, \dots, n$. This means that B_i is finitely generated and projective as an A-module for every $i = 1, \dots, n$. By lemma 2.1.37, this implies that $\bigoplus_{i=1}^n B_i$ is finitely generated and projective as an A-module. So B is a finite projective A-algebra.
Conversely, assume that B is a finite projective A-algebra, i.e. $\bigoplus_{i=1}^n B_i$ is finitely generated and projective as an A-module. By corollary 2.1.10, it follows that B_i is a projective A-module for every $i = 1, \dots, n$. Fix $j \in I$ and consider the projection $p_j : \bigoplus_{i=1}^n B_i \to B_j$, $(x_1, \dots, x_n) \mapsto x_j$, which is A-linear and surjective. Then, if $(v_1, \dots, v_n)$ generates $\bigoplus_{i=1}^n B_i$ as an A-module, we have that $(p_j(v_1), \dots, p_j(v_n))$ generates B_j as an A-module. So B_j is finitely generated. This shows that B_j is a finite projective A-algebra. □

Lemma 2.1.53. *Let B be an A-algebra and P a B-module. Consider the induced A-module structure on P. Then:*

(1) if P is finitely generated over B and B is finitely generated as an A-module, then P is finitely generated over A;

(2) if P is projective over B and B is projective as an A-module, then P is projective over A.

Proof. (1) Let $(w_1, \ldots, w_n)$ and $(v_1, \ldots, v_m)$ be respectively a set of generators of P over B and a set of generators of B as an A-module ($n, m \in \mathbb{N}$). Let $x \in P$. Then there exist $b_1, \ldots, b_n \in B$ such that $x = \sum_{i=1}^{n} b_i w_i$. For any $i = 1, \ldots, n$, there exist $a_{i1}, \ldots, a_{im} \in A$ such that $b_i = \sum_{j=1}^{m} a_{ij} v_j$. Then

$$x = \sum_{i=1}^{n} b_i w_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} v_j \right) w_i = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} (v_j w_i) .$$

This shows that $(v_j w_i)_{i=1,\ldots,n,\, j=1,\ldots,m}$ generates P over A. Then P is finitely generated as an A-module.

(2) Since P is projective as a B-module, by lemma 2.1.14 ((i) $\Longrightarrow$ (iv)) there exists a B-module Q such that $P \oplus Q$ is a free B-module, i.e. $P \oplus Q \cong \bigoplus_{i \in I} B$ as B-modules, for some index set I. We can consider also on Q the induced A-module structure. Then, since any B-linear map is also A-linear, we have that $P \oplus Q \cong \bigoplus_{i \in I} B$ also as A-modules. Since B is a projective A-module, by corollary 2.1.10 we have that $P \oplus Q \cong \bigoplus_{i \in I} B$ is projective over A. Then, applying again the same corollary, P is projective over A.

□

Corollary 2.1.54. *Let B be a finite projective A-algebra and C a finite projective B-algebra. Consider the induced A-algebra structure on C. Then C is a finite projective A-algebra.*

Proof. It follows immediately from lemma 2.1.53. □

We want now to describe the behaviour of finitely generated projective A-modules under extensions of the scalar ring (then the same result will obviously be true for finite projective A-algebras).

Lemma 2.1.55. *Let M, N be A-modules and let B be a flat A-algebra. Define the map*

$$\varphi_{M,N} : \mathrm{Hom}_A(M, N) \otimes_A B \to \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B),\ f \otimes b \mapsto f \otimes (b\, \mathrm{id}_B) .$$

We have that $\varphi_{M,N}$ is an isomorphism of B-modules if one of the following two conditions is satisfied:

(1) M is finitely presented and B is flat as an A-module;

(2) M is finitely generated and projective.

Proof. First of all, we check that $\varphi_{M,N}$ is well defined. For any $b \in B$, $f \in \mathrm{Hom}_A(M,N)$, the map $f \otimes (b\,\mathrm{id}_B) : M \otimes_A B \to N \otimes_A B$ is clearly B-linear, i.e. $f \otimes (b\,\mathrm{id}_B) \in \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$. So we can consider the map

$$\Phi_{M,N} : \mathrm{Hom}_A(M,N) \times B \to \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B),\ (f,b) \mapsto f \otimes (b\,\mathrm{id}_B)\ .$$

It is immediate to prove that $\Phi_{M,N}$ is A-bilinear. So it induces an A-linear map $\varphi_{M,N}$ as in the statement. We prove now that $\varphi_{M,N}$ is also B-linear. Let $f \in \mathrm{Hom}_A(M,N)$, $b \in B$ and $\lambda \in B$. We have that $\varphi_{M,N}(\lambda(f \otimes b)) = \varphi_{M,N}(f \otimes (\lambda b)) = f \otimes ((\lambda b)\,\mathrm{id}_B) = f \otimes (\lambda(b\,\mathrm{id}_B))$. Moreover, for any $x \in M$, $y \in B$, we have

$$(f \otimes (\lambda(b\,\mathrm{id}_B)))(x \otimes y) = f(x) \otimes (\lambda(by)) = \lambda(f(x) \otimes (by)) = \lambda(f \otimes (b\,\mathrm{id}_B))(x \otimes y)\ .$$

So $\varphi_{M,N}(\lambda(f \otimes b)) = f \otimes (\lambda(b\,\mathrm{id}_B)) = \lambda(f \otimes (b\,\mathrm{id}_B))$. Since $\varphi_{M,N}$ is A-linear, we get that $\varphi_{M,N}(\lambda x) = \lambda\varphi_{M,N}(x)$ for any $\lambda \in B$, $x \in \mathrm{Hom}_A(M,N) \otimes_A B$, i.e. $\varphi_{M,N}$ is B-linear.

We prove now that $\varphi_{M,N}$ is an isomorphism when $M = A^n$ for some $n \in \mathbb{N}$ (with no assumption on B). We have a canonical isomorphism of A-modules $\vartheta : \mathrm{Hom}_A(A^n, N) \to N^n$, $f \mapsto (f(e_1), \ldots, f(e_n))$, where $(e_1, \ldots, e_n)$ is the canonical basis of A^n. This leads to an isomorphism of B-modules $\vartheta \otimes \mathrm{id}_B : \mathrm{Hom}_A(A^n, N) \otimes_A B \to N^n \otimes_A B$. Lemma 2.1.19 gives us an isomorphism of A-modules $\psi_B : N^n \otimes_A B \to (N \otimes_A B)^n$, which is easily seen to be B-linear. So

$$\psi_B \circ (\vartheta \otimes \mathrm{id}_B) : \mathrm{Hom}_A(A^n, N) \otimes_A B \to (N \otimes_A B)^n$$

is an isomorphism of B-modules. On the other hand, lemma 2.1.19 gives also an isomorphism of A-modules $\psi'_B : A^n \otimes_A B \to (A \otimes_A B)^n$ and also this one is easily seen to be B-linear and then an isomorphism of B-modules. We have a canonical isomorphism of B modules $\sigma : A \otimes_A B \to B$, $a \otimes b \mapsto ab$, which induces an isomorphism of B-modules $\bigoplus_{i=1}^n \sigma : (A \otimes_A B)^n \to B^n$. So $(\bigoplus_{i=1}^n \sigma) \circ \psi'_B : A^n \otimes_A B \to B^n$ is an isomorphism of B-modules. Its inverse induces an isomorphism of B-modules $\left((\psi'_B)^{-1} \circ (\bigoplus_{i=1}^n \sigma)^{-1}\right)^* : \mathrm{Hom}_B(A^n \otimes_A B, N \otimes_A B) \to \mathrm{Hom}_B(B^n, N \otimes_A B)$. Finally, we have a canonical isomorphism of B-modules $\vartheta' : \mathrm{Hom}_B(B^n, N \otimes_A B) \to (N \otimes_A B)^n$, $f \mapsto (f(e'_1), \ldots, f(e'_n))$, where $(e'_1, \ldots, e'_n)$ is the canonical basis of B^n (notice that $e'_i = ((\bigoplus_{i=1}^n \sigma) \circ \psi'_B)(e_i \otimes 1)$, for any $i = 1, \ldots, n$). So

$$\vartheta' \circ \left((\psi'_B)^{-1} \circ \left(\bigoplus_{i=1}^n \sigma \right)^{-1} \right)^* : \mathrm{Hom}_B(A^n \otimes_A B, N \otimes_A B) \to (N \otimes_A B)^n$$

is an isomorphism of B-modules. Consider now the following diagram.

$$\begin{array}{ccc}
\mathrm{Hom}_A(A^n, N) \otimes_A B & \xrightarrow{\varphi_{A^n,N}} & \mathrm{Hom}_B(A^n \otimes_A B, N \otimes_A B) \\
\Big\downarrow {\scriptstyle \psi_B \circ (\vartheta \otimes \mathrm{id}_B)} & & \Big\downarrow {\scriptstyle \vartheta' \circ \left((\psi'_B)^{-1} \circ (\bigoplus_{i=1}^n \sigma)^{-1}\right)^*} \\
(N \otimes_A B)^n & \xrightarrow{\mathrm{id}_{(N \otimes_A B)^n}} & (N \otimes_A B)^n
\end{array}$$

Let $f \in \mathrm{Hom}_A(A^n, N)$, $b \in B$. We have that

$$\begin{aligned}
&(\psi_B \circ (\vartheta \otimes \mathrm{id}_B))(f \otimes b) = \psi_B(\vartheta(f) \otimes b) = \psi_B((f(e_1), \ldots, f(e_n)) \otimes b) = \\
&= (f(e_1) \otimes b, \ldots, f(e_n) \otimes b) = ((f \otimes (b\,\mathrm{id}_B))(e_1 \otimes 1), \ldots, (f \otimes (b\,\mathrm{id}_B))(e_n \otimes 1)) = \\
&= \left(\left((f \otimes (b\,\mathrm{id}_B)) \circ (\psi'_B)^{-1} \circ \left(\bigoplus_{i=1}^n \sigma \right)^{-1} \right) (e'_i) \right)_{i=1,\ldots,n} = \\
&= \vartheta' \left((f \otimes (b\,\mathrm{id}_B)) \circ (\psi'_B)^{-1} \circ \left(\bigoplus_{i=1}^n \sigma \right)^{-1} \right) = \\
&= \left(\vartheta' \circ \left((\psi'_B)^{-1} \circ \left(\bigoplus_{i=1}^n \sigma \right)^{-1} \right)^* \right) (f \otimes (b\,\mathrm{id}_B)) = \\
&= \left(\vartheta' \circ \left((\psi'_B)^{-1} \circ \left(\bigoplus_{i=1}^n \sigma \right)^{-1} \right)^* \circ \varphi_{A^n,N} \right) (f \otimes b) .
\end{aligned}$$

So $\psi_B \circ (\vartheta \otimes \mathrm{id}_B) = \vartheta' \circ \left((\psi'_B)^{-1} \circ (\bigoplus_{i=1}^n \sigma)^{-1} \right)^* \circ \varphi_{A^n,N}$, i.e. the diagram is commutative. Since $(\psi_B \circ (\vartheta \otimes \mathrm{id}_B))$ and $\vartheta' \circ \left((\psi'_B)^{-1} \circ (\bigoplus_{i=1}^n \sigma)^{-1} \right)^*$ are isomorphisms, it follows that $\varphi_{A^n,N}$ is bijective.

Assume now that the condition (1) is satisfied. Since M is finitely presented, there exists an exact sequence $A^m \xrightarrow{\alpha} A^n \xrightarrow{\beta} M \to 0$, with $m, n \in \mathbb{N}$. Since B is flat, the sequence (of B-modules) $A^m \otimes_A B \xrightarrow{\alpha \otimes \mathrm{id}_B} A^n \otimes_A B \xrightarrow{\beta \otimes \mathrm{id}_B} M \otimes_A B \to 0 \otimes_A B = 0$ is also exact. Recall that the contravariant functor $\mathrm{Hom}_B(-, P) : \mathbf{Mod}_B \to \mathbf{Mod}_B$ is left exact for any B-module P. In particular, this holds for $P = N \otimes_A B$. So the sequence

$$\begin{aligned}
0 \to \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B) \xrightarrow{(\beta \otimes \mathrm{id}_B)^*} \mathrm{Hom}_B(A^n \otimes_A B, N \otimes_A B) \xrightarrow{(\alpha \otimes \mathrm{id}_B)^*} \\
\xrightarrow{(\alpha \otimes \mathrm{id}_B)^*} \mathrm{Hom}_B(A^m \otimes_A B, N \otimes_A B) ,
\end{aligned}$$

where we defined $(\beta \otimes \mathrm{id}_B)^*$ and $(\alpha \otimes \mathrm{id}_B)^*$ in the obvious way, is exact. On the other hand, applying left-exactness of the contravariant functor $\mathrm{Hom}_A(-, N) : \mathbf{Mod}_A \to \mathbf{Mod}_A$, we get that the sequence

$$0 \to \mathrm{Hom}_A(M, N) \xrightarrow{\beta^*} \mathrm{Hom}_A(A^n, N) \xrightarrow{\alpha^*} \mathrm{Hom}_A(A^m, N)$$

is exact, where α^* and β^* are defined in the obvious way. Since B is flat, the sequence

$$\begin{aligned}
0 \to \mathrm{Hom}_A(M, N) \otimes_A B \xrightarrow{\beta^* \otimes \mathrm{id}_B} \mathrm{Hom}_A(A^n, N) \otimes_A B \xrightarrow{\alpha^* \otimes \mathrm{id}_B} \\
\xrightarrow{\alpha^* \otimes \mathrm{id}_B} \mathrm{Hom}_A(A^m, N) \otimes_A B
\end{aligned}$$

is also exact. Consider now the following diagram.

$$\begin{array}{ccc}
 & & \\
 0 & & 0 \\
 \downarrow & & \downarrow \\
 \mathrm{Hom}_A(M,N)\otimes_A B & \xrightarrow{\varphi_{M,N}} & \mathrm{Hom}_B(M\otimes_A B, N\otimes_A B) \\
 \beta^*\otimes \mathrm{id}_B \downarrow & & \downarrow (\beta\otimes \mathrm{id}_B)^* \\
 \mathrm{Hom}_A(A^n,N)\otimes_A B & \xrightarrow{\varphi_{A^n,N}} & \mathrm{Hom}_B(A^n\otimes_A B, N\otimes_A B) \\
 \alpha^*\otimes \mathrm{id}_B \downarrow & & \downarrow (\alpha\otimes \mathrm{id}_B)^* \\
 \mathrm{Hom}_A(A^m,N)\otimes_A B & \xrightarrow{\varphi_{A^m,N}} & \mathrm{Hom}_B(A^m\otimes_A B, N\otimes_A B)
\end{array}$$

For any $f \in \mathrm{Hom}_A(M,N)$, $b \in B$, we have that

$$\begin{aligned}
\varphi_{A^n,N}((\beta^*\otimes \mathrm{id}_B)(f\otimes b)) &= \varphi_{A^n,N}(\beta^*(f)\otimes b) = \varphi_{A^n,N}((f\circ\beta)\otimes b) = \\
&= (f\circ\beta)\otimes(b\,\mathrm{id}_B) = (f\otimes(b\,\mathrm{id}_B))\circ(\beta\otimes \mathrm{id}_B) = \\
&= (\beta\otimes \mathrm{id}_B)^*(f\otimes(b\,\mathrm{id}_B)) = (\beta\otimes \mathrm{id}_B)^*(\varphi_{M,N}(f\otimes b)) \ .
\end{aligned}$$

So $\varphi_{A^n,N}\circ(\beta^*\otimes \mathrm{id}_B) = (\beta\otimes \mathrm{id}_B)^*\circ\varphi_{M,N}$ (by linearity, it is enough to check equality on pure tensors). In the same way, one proves that $\varphi_{A^m,N}\circ(\alpha^*\otimes \mathrm{id}_B) = (\alpha\otimes \mathrm{id}_B)^*\circ\varphi_{A^n,N}$. So the diagram is commutative. By what we proved above, $\varphi_{A^n,N}$ and $\varphi_{A^m,N}$ are bijective. Now we have that $(\beta\otimes \mathrm{id}_B)^*\circ\varphi_{M,N} = (\beta^*\otimes \mathrm{id}_B)\circ\varphi_{A^n,N}$ is injective, because it is the composition of injective functions. So $\varphi_{M,N}$ must be injective.
On the other hand, let $f \in \mathrm{Hom}_B(M\otimes_A B, N\otimes_A B)$. Consider $(\beta\otimes \mathrm{id}_B)^*(f) \in \mathrm{Hom}_B(A^n\otimes_A B, N\otimes_A B)$. Since $\varphi_{A^n,N} : \mathrm{Hom}_A(A^n,N)\otimes_A B \to \mathrm{Hom}_B(A^n\otimes_A B, N\otimes B)$ is surjective, there exists $y \in \mathrm{Hom}_A(A^n,N)\otimes_A B$ such that $(\beta\otimes\mathrm{id}_B)^*(f) = \varphi_{A^n,N}(y)$. By the exactness we proved above, we have that $(\alpha\otimes\mathrm{id}_B)^*\circ(\beta\otimes\mathrm{id}_B)^* = 0$. Then

$$0 = (\alpha\otimes \mathrm{id}_B)^*((\beta\otimes \mathrm{id}_B)^*(f)) = (\alpha\otimes \mathrm{id}_B)^*(\varphi_{A^n,N}(y)) = \varphi_{A^m,N}((\alpha^*\otimes \mathrm{id}_B)(y)) \ .$$

Since $\varphi_{A^m,N}$ is injective, it follows that $(\alpha^*\otimes \mathrm{id}_B)(y) = 0$, i.e. $y \in \mathrm{Ker}(\alpha^*\otimes \mathrm{id}_B)$. By the exactness we proved above, we have that $\mathrm{Ker}(\alpha^*\otimes \mathrm{id}_B) = \mathrm{Im}(\beta^*\otimes \mathrm{id}_B)$. So there exists $x \in \mathrm{Hom}_A(M,N)\otimes_A B$ such that $y = (\beta^*\otimes \mathrm{id}_B)(x)$. Then

$$(\beta\otimes \mathrm{id}_B)^*(f) = \varphi_{A^n,N}(y) = \varphi_{A^n,N}((\beta^*\otimes \mathrm{id}_B)(x)) = (\beta\otimes \mathrm{id}_B)^*(\varphi_{M,N}(x)) \ .$$

But $(\beta\otimes\mathrm{id}_B)^*$ is injective (by exactness of the corresponding sequence). So we must have $f = \varphi_{M,N}(x)$. Hence $\varphi_{M,N}$ is surjective.
Assume instead that the condition (2) is satisfied, i.e. that M is finitely generated and projective. By corollary 2.1.15, there exist an A-module Q and an $n \in \mathbb{N}$ such that $M \oplus Q \cong A^n$. Let $\gamma : A^n \to M\oplus Q$ be an isomorphism of A-modules, $p_M : M\oplus Q \to M$ and $p_Q : M\oplus Q \to Q$ the canonical projections, $i_M : M \to M\oplus Q$, $x \mapsto (x,0)$ and $i_Q : Q \to M\oplus Q$, $y \mapsto (0,y)$. Then the sequence

$$0 \to Q \xrightarrow{\gamma^{-1}\circ i_Q} A^n \xrightarrow{p_M\circ\gamma} M \to 0$$

is split exact by definition. The functors $-\otimes_A B : \mathbf{Mod}_A \to \mathbf{Mod}_A$, $\mathrm{Hom}_A(-, N) : \mathbf{Mod}_A \to \mathbf{Mod}_A$ and $\mathrm{Hom}_B(-, N \otimes_A B) : \mathbf{Mod}_B \to \mathbf{Mod}_B$ preserve split exact sequences. Applying $-\otimes_A B$ and then $\mathrm{Hom}_B(-, N \otimes_A B)$, we get that the sequence

$$\begin{aligned} 0 \to \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B) \xrightarrow{((p_M \circ \gamma)\otimes \mathrm{id}_B)^*} \mathrm{Hom}_B(A^n \otimes_A B, N \otimes_A B) \\ \xrightarrow{((\gamma^{-1} \circ i_Q)\otimes \mathrm{id}_B)^*} \mathrm{Hom}_B(Q \otimes_A B, N \otimes_A B) \to 0 \end{aligned}$$

is exact. On the other hand, applying first $\mathrm{Hom}_A(-, N)$ and then $-\otimes_A B$, we get that the sequence

$$\begin{aligned} 0 \to \mathrm{Hom}_A(M, N) \otimes_A B \xrightarrow{(p_M \circ \gamma)^* \otimes \mathrm{id}_B} \mathrm{Hom}_A(A^n, N) \otimes_A B \xrightarrow{(\gamma^{-1} \circ i_Q)^* \otimes \mathrm{id}_B} \\ \xrightarrow{(\gamma^{-1} \circ i_Q)^* \otimes \mathrm{id}_B} \mathrm{Hom}_A(Q, N) \otimes_A B \to 0 \end{aligned}$$

is exact. Consider now the following diagram.

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ \mathrm{Hom}_A(M, N) \otimes_A B & \xrightarrow{\varphi_{M,N}} & \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B) \\ {\scriptstyle (p_M \circ \gamma)^* \otimes \mathrm{id}_B} \downarrow & & \downarrow {\scriptstyle ((p_M \circ \gamma) \otimes \mathrm{id}_B)^*} \\ \mathrm{Hom}_A(A^n, N) \otimes_A B & \xrightarrow{\varphi_{A^n,N}} & \mathrm{Hom}_B(A^n \otimes_A B, N \otimes_A B) \\ {\scriptstyle (\gamma^{-1} \circ i_Q)^* \otimes \mathrm{id}_B} \downarrow & & \downarrow {\scriptstyle ((\gamma^{-1} \circ i_Q) \otimes \mathrm{id}_B)^*} \\ \mathrm{Hom}_A(Q, N) \otimes_A B & \xrightarrow{\varphi_{Q,N}} & \mathrm{Hom}_B(Q \otimes_A B, N \otimes_A B) \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array}$$

Commutativity of the diagram can be proved as above. We know that $\varphi_{A^n,N}$ is an isomorphism. Then $((p_M \circ \gamma) \otimes \mathrm{id}_B)^* \circ \varphi_{M,N} = \varphi_{A^n,N} \circ ((p_M \circ \gamma)^* \otimes \mathrm{id}_B)$ is injective, because it is a composition of injective maps. So $\varphi_{M,N}$ must be injective. If we start with the split exact sequence

$$0 \to M \xrightarrow{\gamma^{-1} \circ i_M} A^n \xrightarrow{p_Q \circ \gamma} Q \to 0$$

and apply the same argument, we get that $\varphi_{M,N} \circ ((\gamma^{-1} \circ i_M)^* \otimes \mathrm{id}_B) = ((\gamma^{-1} \circ i_M) \otimes \mathrm{id}_B)^* \circ \varphi_{A^n,N}$ is surjective, because it is a composition of surjective maps. So $\varphi_{M,N}$ must be surjective. Hence $\varphi_{M,N}$ is an isomorphism. □

Remark 2.1.56. Notice that lemma 2.1.55 (with the condition (1)) is a generalization of lemma 2.1.27, because localization at S coincides with tensor product with $S^{-1}A$ (which is a flat A-algebra, see [3], proposition 3.3), for any multiplicative subset $S \subseteq A$.

Proposition 2.1.57. *Let B be a faithfully flat A-algebra and P an A-module. Then P is finitely generated and projective as an A-module if and only if $P \otimes_A B$ is finitely generated and projective as a B-module.*

Proof. Assume that P is finitely generated and projective as an A-module. By lemma 2.1.24, $P \otimes_A B$ is a projective B-module. Moreover, if $(w_1, \dots, w_n)$ generates P over A, then $(w_1 \otimes 1, \dots, w_n \otimes 1)$ generates $P \otimes_A B$ over B. So $P \otimes_A B$ is finitely generated over B.
Conversely, assume that $P \otimes_A B$ is finitely generated and projective as a B-module. Let $(w_1, \dots, w_n)$ be a set of generators of $P \otimes_A B$ over B. By definition of tensor product, for any $i = 1, \dots, n$ there exist $m_i \in \mathbb{N}$, $p_{i1}, \dots, p_{im_i} \in P$, $b_{i1}, \dots, b_{im_i} \in B$ such that $w_i = \sum_{j=1}^{m_i} p_{ij} \otimes b_{ij}$. Let $x \in P \otimes_A B$. Since $(w_1, \dots, w_n)$ generates $P \otimes_A B$ over B, there exist $\lambda_1, \dots, \lambda_n \in B$ such that $x = \lambda_1 w_1 + \dots + \lambda_n w_n$. Then

$$x = \sum_{i=1}^{n} \lambda_i w_i = \sum_{i=1}^{n} \lambda_i \sum_{j=1}^{m_i} p_{ij} \otimes b_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{m_i} \lambda_i b_{ij} (p_{ij} \otimes 1) \ .$$

So $(p_{ij} \otimes 1)_{i=1,\dots,n,\, j=1,\dots,m_i}$ generates $P \otimes_A B$ over B. Let $F := \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} A$, with canonical basis $(e_{ij})_{i=1,\dots,n,\, j=1,\dots,m_i}$ and define an A-linear map $f : F \to P$ by $f(e_{ij}) = p_{ij}$ for any $i = 1, \dots, n$, $j = 1, \dots, m_i$, extended by linearity. Consider the B-linear map $f \otimes \mathrm{id}_B : F \otimes_A B \to P \otimes_A B$. For any $i = 1, \dots, n$, $j = 1, \dots, m_i$, we have that $(f \otimes \mathrm{id}_B)(e_{ij} \otimes 1) = p_{ij} \otimes 1$. Since $(p_{ij} \otimes 1)_{i=1,\dots,n,\, j=1,\dots,m_i}$ generates $P \otimes_A B$ over B, we have that $f \otimes \mathrm{id}_B$ is surjective. So the sequence

$$F \otimes_A B \xrightarrow{f \otimes \mathrm{id}_B} P \otimes_A B \to 0 = 0 \otimes_A B$$

is exact. Since B is faithfully flat, this implies that the sequence $F \xrightarrow{f} P \to 0$ is exact, i.e. f is surjective. Then $(f(e_{ij}) = p_{ij})_{i=1,\dots,n,\, j=1,\dots,m_i}$ is a set of generators of P over A and so P is finitely generated. We prove now that P is finitely presented (this will allow us to apply lemma 2.1.55). Define $Q := \mathrm{Ker}(f)$. Then the sequence $0 \to Q \xrightarrow{\iota} F \xrightarrow{f} P \to 0$, where $\iota : Q \to F$ is the canonical inclusion. Since B is flat, the sequence of B-modules

$$0 \to Q \otimes_A B \xrightarrow{\iota \otimes \mathrm{id}_B} F \otimes_A B \xrightarrow{f \otimes \mathrm{id}_B} P \otimes_A B \to 0$$

is also exact. But $P \otimes_A B$ is a projective B-module, so the sequence splits, by lemma 2.1.14 ((i) $\Longrightarrow$ (iii)). Then

$$(Q \otimes_A B) \oplus (P \otimes_A B) \cong F \otimes_A B = \left(\bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} A \right) \otimes_A B \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} B \ ,$$

which is free. By lemma 2.1.14 ((iv) $\Longrightarrow$ (i)), $Q \otimes_A B$ is a projective B-module. Moreover, if $\varphi : \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} B \to (Q \otimes_A B) \oplus (P \otimes_A B)$ is an isomorphism and $p_1 : (Q \otimes_A B) \oplus (P \otimes_A B) \to Q \otimes_A B$ is the canonical projection, we have that $p_1 \circ \varphi : \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} B \to Q \otimes_A B$ is a surjective B-linear map. Then $((p_1 \circ \varphi)(e'_{ij}))_{i=1,\dots,n,\, j=1,\dots,m_i}$ generates $Q \otimes_A B$ over B, where $(e'_{ij})_{i=1,\dots,n,\, j=1,\dots,m_i}$ is the

canonical basis of $\bigoplus_{i=1}^{n}\bigoplus_{j=1}^{m_i} B$. So $Q\otimes_A B$ is finitely generated over B. Then we can apply the same argument we applied above to $P\otimes_A B$ and conclude that Q is finitely generated. So P is finitely presented (see remark 2.1.26).
Let now M, N be A-modules and $g: M\to N$ a surjective A-linear map. Then the sequence $M\xrightarrow{g} N\to 0$ is exact. Since B is flat, it follows that the sequence $M\otimes_A B\xrightarrow{g\otimes \mathrm{id}_B} N\otimes_A B\to 0\otimes_A B=0$ is also exact, i.e. the B-linear map $g\otimes\mathrm{id}_B: M\otimes_A B\to N\otimes_A B$ is surjective. Then, by lemma 2.1.14 ((i) $\Longrightarrow$ (ii)), we have that the map

$$(g\otimes\mathrm{id}_B)_*:\mathrm{Hom}_B(P\otimes_A B, M\otimes_A B)\to \mathrm{Hom}_B(P\otimes_A B, N\otimes_A B),\ h\mapsto (g\otimes\mathrm{id}_B)\circ h$$

is surjective. Since P is finitely presented and B is flat, by lemma 2.1.55 we have isomorphisms $\varphi_{P,M}:\mathrm{Hom}_A(P,M)\otimes_A B\to\mathrm{Hom}_B(P\otimes_A B, M\otimes_A B)$ and $\varphi_{P,N}:\mathrm{Hom}_A(P,N)\otimes_A B\to\mathrm{Hom}_B(P\otimes_A B, N\otimes_A B)$. Consider the following diagram, where we defined $g_*:\mathrm{Hom}_A(P,M)\to\mathrm{Hom}_A(P,N)$, $h\mapsto g\circ h$.

$$\begin{array}{ccc} \mathrm{Hom}_A(P,M)\otimes_A B & \xrightarrow{\varphi_{P,M}} & \mathrm{Hom}_B(P\otimes_A B, M\otimes_A B) \\ {\scriptstyle g_*\otimes\mathrm{id}_B}\downarrow & & \downarrow{\scriptstyle (g\otimes\mathrm{id}_B)_*} \\ \mathrm{Hom}_A(P,N)\otimes_A B & \xrightarrow{\varphi_{P,N}} & \mathrm{Hom}_B(P\otimes_A B, N\otimes_A B) \end{array}$$

For any $f\in\mathrm{Hom}_A(P,M)$, $b\in B$, we have that

$$\varphi_{P,N}((g_*\otimes\mathrm{id}_B)(f\otimes b))=\varphi_{P,N}(g_*(f)\otimes b)=\varphi_{P,N}((g\circ f)\otimes b)=(g\circ f)\otimes(b\,\mathrm{id}_B)=$$
$$=(g\otimes\mathrm{id}_B)\circ(f\otimes(b\,\mathrm{id}_B))=(g\otimes\mathrm{id}_B)_*(f\otimes(b\,\mathrm{id}_B))=(g\otimes\mathrm{id}_B)_*(\varphi_{P,M}(f\otimes b))\ .$$

So the diagram commutes, i.e. $\varphi_{P,N}\circ(g_*\otimes\mathrm{id}_B)=(g\otimes\mathrm{id}_B)_*\circ\varphi_{P,M}$ (by linearity it is enough to check equality on pure tensors). Then we have that $g_*\otimes\mathrm{id}_B=\varphi_{P,N}^{-1}\circ(g\otimes\mathrm{id}_B)_*\circ\varphi_{P,M}$ is surjective, because $(g\otimes\mathrm{id}_B)_*$ is surjective and $\varphi_{P,M}$ and $\varphi_{P,N}$ are isomorphisms. Then the sequence

$$\mathrm{Hom}_A(P,M)\otimes_A B\xrightarrow{g_*\otimes\mathrm{id}_B}\mathrm{Hom}_A(P,N)\otimes_A B\to 0=0\otimes_A B$$

is exact. Since B is faithfully flat, we get that the sequence $\mathrm{Hom}_A(P,M)\xrightarrow{g}\mathrm{Hom}_A(P,N)\to 0$ is exact, i.e. g is surjective. By lemma 2.1.14 ((ii) $\Longrightarrow$ (i)), we have that P is a projective A-module. □

The following result illustrates the importance of the rank $[B:A]$. We will write shortly $[B:A]\geq 1$ (respectively, $[B:A]\leq 1$ or $[B:A]=1$) to say that $[B:A](\mathfrak{p})\geq 1$ (respectively, $[B:A](\mathfrak{p})\leq 1$ or $[B:A](\mathfrak{p})=1$) for any $\mathfrak{p}\in\mathrm{Spec}(A)$.

Lemma 2.1.58. *Let B be a finite projective A-algebra. Consider the corresponding ring homomorphism $\varphi: A\to B$ (which is of course also an A-algebra homomorphism). We have that:*

(1) φ is injective if and only if $[B:A]\geq 1$ (i.e. if and and only if B is faithfully projective, see the definition 2.1.51(2));

(2) *φ is surjective if and only if $[B : A] \leq 1$, and if and only if the map $m : B \otimes_A B \to B$, $x \otimes y \mapsto xy$ (extended by linearity) is an isomorphism of A-algebras;*

(3) *φ is an isomorphism if and only if $[B : A] = 1$.*

Proof. (1) Let φ be injective and assume by contradiction that there exists $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $[B : A](\mathfrak{p}) < 1$. Then $[B : A](\mathfrak{p}) = 0$ (recall that $[B : A](\mathfrak{p})$ is a non-negative integer by definition). This means that $\mathrm{rank}_{A_\mathfrak{p}}(B_\mathfrak{p}) = 0$, i.e. $B_\mathfrak{p} = 0$. Then $\varphi_\mathfrak{p} : A_\mathfrak{p} \to 0 = B_\mathfrak{p}$ cannot be injective (notice that $A_\mathfrak{p} \neq 0$, because $\frac{1}{1} \neq \frac{0}{1}$). This is a contradiction, by lemma 2.1.28(2).
Conversely, assume that $[B : A] \geq 1$. Let $\mathfrak{p} \in \mathrm{Spec}(A)$. By corollary 2.1.33(2), we have that $B_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module. Let $(w_1, \ldots, w_n)$ be a basis of $B_\mathfrak{p}$ over $A_\mathfrak{p}$, with $n = \mathrm{rank}_{A_\mathfrak{p}}(B_\mathfrak{p}) = [B : A](\mathfrak{p}) \geq 1$. Let $x = \frac{a}{s} \in \mathrm{Ker}(\varphi_\mathfrak{p}) \subseteq A_\mathfrak{p}$, i.e. $\frac{\varphi(a)}{s} = \varphi_\mathfrak{p}(x) = 0$. This means that there exists $u \in A \backslash \mathfrak{p}$ such that $u\varphi(a) = 0$. Then for any $y = \frac{b}{t} \in B_\mathfrak{p}$ we have that $xy = \frac{a}{s}\frac{b}{t} = \frac{ab}{st} = \frac{\varphi(a)b}{st} = 0$, because $u\varphi(a)b = 0$. In particular, $xw_1 = 0$. But $(w_1, \ldots, w_n)$ is linearly independent over $A_\mathfrak{p}$. So we must have $x = 0$. Then $\mathrm{Ker}(\varphi_\mathfrak{p}) = 0$, i.e. $\varphi_\mathfrak{p}$ is injective. Since this holds for any prime ideal $\mathfrak{p}$, we have that φ is injective by lemma 2.1.28(2).

(2) First of all, notice that m is well defined and A-linear, because the multiplication in B is A-bilinear. Moreover, by definition of the ring structure on $B \otimes_A B$, we have that m is also a ring homomorphism. So m is a homomorphism of A-algebras.
Assume that m is an isomorphism. The rank is clearly invariant by isomorphism. So we must have $[B \otimes_A B : A] = [B : A]$. By lemma 2.1.40, we have that $[B \otimes_A B : A] = \mathrm{rank}_A(B \otimes_A B) = \mathrm{rank}_A(B)^2 = [B : A]^2$. So, for any $\mathfrak{p} \in \mathrm{Spec}(A)$, we have that

$$([B : A](\mathfrak{p}))^2 = [B \otimes_A B : A](\mathfrak{p}) = [B : A](\mathfrak{p}) \ ,$$

which implies that $[B : A](\mathfrak{p}) \in \{0, 1\}$. So $[B : A] \leq 1$.
Suppose now that $[B : A] \leq 1$. Let $\mathfrak{p} \in \mathrm{Spec}(A)$. Since $\mathrm{rank}_{A_\mathfrak{p}}(B_\mathfrak{p}) = [B : A](\mathfrak{p}) \geq 1$, we have that either $\mathrm{rank}_{A_\mathfrak{p}}(B_\mathfrak{p}) = 0$ or $\mathrm{rank}_{A_\mathfrak{p}}(B_\mathfrak{p}) = 1$ (because by definition it must be a non-negative integer). In the first case we have that $B_\mathfrak{p} = 0$ and so $\varphi_\mathfrak{p} : A_\mathfrak{p} \to B_\mathfrak{p} = 0$ must be surjective. If instead $\mathrm{rank}_{A_\mathfrak{p}}(B_\mathfrak{p}) = 1$, let w be a generator of $B_\mathfrak{p}$ over $A_\mathfrak{p}$. Let $x = \frac{b}{s} \in B_\mathfrak{p}$. The A-linear map $m_b : B \to B$, $y \mapsto by$ induces an $A_\mathfrak{p}$-linear map $(m_b)_\mathfrak{p} : B_\mathfrak{p} \to B_\mathfrak{p}$. Define $\psi_x := \frac{1}{s}(m_b)_\mathfrak{p}$. Consider $\psi_x(w) \in B_\mathfrak{p}$. Since w generates $B_\mathfrak{p}$ over $A_\mathfrak{p}$, there exists $\lambda_x \in A_\mathfrak{p}$ such that $\psi_x(w) = \lambda_x w$. By definition of $A_\mathfrak{p}$, there exist $a \in A$, $u \in A \backslash \mathfrak{p}$ such that $\lambda_x = \frac{a}{u}$. Consider $\frac{1}{1} \in B_\mathfrak{p}$. Since w generates $B_\mathfrak{p}$ over $A_\mathfrak{p}$, there exists $\lambda \in A_\mathfrak{p}$ such that $\frac{1}{1} = \lambda w$. Then, since ψ_x is $A_\mathfrak{p}$-bilinear, we have that

$$\psi_x\left(\frac{1}{1}\right) = \psi_x(\lambda w) = \lambda \psi_x(w) = \lambda(\lambda_x w) = \lambda_x(\lambda w) = \frac{a}{u}\frac{1}{1} = \frac{a \cdot 1}{u} = \frac{\varphi(a)}{u} \ .$$

On the other hand, by definition of ψ_x, we have that

$$\psi_x\left(\frac{1}{1}\right)=\frac{1}{s}(m_b)_{\mathfrak{p}}\left(\frac{1}{1}\right)=\frac{1}{s}\frac{m_b(1)}{1}=\frac{1}{s}\frac{b\cdot 1}{1}=\frac{b}{s}\ .$$

So $x=\frac{b}{s}=\frac{\varphi(a)}{u}=\varphi_{\mathfrak{p}}\left(\frac{a}{u}\right)=\varphi_{\mathfrak{p}}(\lambda_x)$. This proves that $\varphi_{\mathfrak{p}}$ is surjective. So $\varphi_{\mathfrak{p}}$ is surjective for any prime ideal $\mathfrak{p}$. By lemma 2.1.28(2), φ is surjective.
Finally, assume that φ is surjective and let us prove that m is bijective. It is clear that m is surjective, because for any $b\in B$ we have $b=m(b\otimes 1)$. Let $x_1\otimes y_1+\cdots+x_n\otimes y_n\in \mathrm{Ker}(m)$. Since $\varphi : A\to B$ is surjective, for any $i=1,\dots,n$ there exists $a_i\in A$ such that $y_i=\varphi(a_i)$. Then

$$\begin{aligned}x_1\otimes y_1+\cdots+x_n\otimes y_n&=x_1\otimes\varphi(a_1)+\cdots+x_n\otimes\varphi(a_n)=\\&=x_1\otimes(a_1\cdot 1)+\cdots+x_n\otimes(a_n\cdot 1)=a_1(x_1\otimes 1)+\cdots+a_n(x_n\otimes 1)=\\&=(a_1x_1)\otimes 1+\cdots+(a_nx_n)\otimes 1=(a_1x_1+\cdots+a_nx_n)\otimes 1\ .\end{aligned}$$

Then $0=m(x_1\otimes y_1+\cdots+x_n\otimes y_n)=m((a_1x_1+\cdots+a_nx_n)\otimes 1)=a_1x_1+\cdots+a_nx_n$, which implies that $x_1\otimes y_1+\cdots+x_n\otimes y_n=0\otimes 1=0$. So $\mathrm{Ker}(m)=0$, i.e. m is injective. Hence m is bijective.

(3) It follows immediately from (1) and (2).

□

We can finally introduce projective separable A-algebras.

Lemma 2.1.59. *Let B be a finite projective A-algebra. For every $b\in B$, define m_b as in lemma 2.1.3. By definition of A-algebra, we have that m_b is A-linear. So we can define $\mathrm{Tr}(b):=\mathrm{Tr}(m_b)$ (as in the definition 2.1.47, we will write $\mathrm{Tr}_{B/A}(b)$ when confusion can arise).*

(1) The map $\mathrm{Tr}: B\to A,\ b\mapsto \mathrm{Tr}(b)$ is A-linear.

(2) The map $\varphi : B\to \mathrm{Hom}_A(B,A),\ x\mapsto (y\mapsto \mathrm{Tr}(xy))$ is A-linear.

Proof. (1) Let $b_1,b_2\in B$, $\lambda_1,\lambda_2\in A$. For any $x\in B$ we have that

$$\begin{aligned}m_{\lambda_1b_1+\lambda_2b_2}(x)&=(\lambda_1b_1+\lambda_2b_2)x=\lambda_1(b_1x)+\lambda_2(b_2x)=\\&=\lambda_1m_{b_1}(x)+\lambda_2m_{b_2}(x)=(\lambda_1m_{b_1}+\lambda_2m_{b_2})(x)\ .\end{aligned}$$

So $m_{\lambda_1b_1+\lambda_2b_2}=\lambda_1m_{b_1}+\lambda_2m_{b_2}$. Then the claim follows from remark 2.1.48.

(2) The proof is identical to the one of lemma 2.1.3(2).

□

Definition 2.1.60. Let B be an A-algebra. We say that B is a *projective separable A-algebra* if B is a finite projective A-algebra and the map φ defined in lemma 2.1.59 is an isomorphism of A-modules.

Remark 2.1.61. The definition 2.1.60 is compatible with the definition 2.1.4, in the sense that an A-algebra is free separable if and only if it is projective separable and free. This follows from remark 2.1.50(3).

To conclude, we prove some results about projective separable A-algebras that we will use in the following sections.

Lemma 2.1.62. *Let $0 \to P_0 \xrightarrow{\alpha} P_1 \xrightarrow{\beta} P_2 \to 0$ be a short exact sequence of A-modules, with P_1 and P_2 finitely generated and projective. Then:*

(1) P_0 is also finitely generated and projective;

(2) if $g : P_1 \to P_1$ is an A-linear map such that $g(\mathrm{Im}(\alpha)) \subseteq \mathrm{Im}(\alpha)$, then

$$\mathrm{Tr}_{P_1/A}(g) = \mathrm{Tr}_{P_0/A}(g_0) + \mathrm{Tr}_{P_2/A}(g_2) ,$$

where $g_0 : P_0 \to P_0$ is the unique A-linear map such that $g \circ \alpha = \alpha \circ g_0$ and $g_2 : P_2 \to P_2$ is the unique A-linear map such that $g_2 \circ \beta = \beta \circ g$.

Proof. (1) Since P_2 is projective, the short exact sequence $0 \to P_0 \xrightarrow{\alpha} P_1 \xrightarrow{\beta} P_2 \to 0$ splits, by lemma 2.1.14 ((i) $\Longrightarrow$ (iii)). So $P_1 \cong P_0 \oplus P_2$. Since P_1 is projective, by corollary 2.1.10 we get that P_0 is projective. Moreover, by lemma 2.1.13, there exists an A-linear map $\gamma : P_1 \to P_0$ such that $\gamma \circ \alpha = \mathrm{id}_{P_0}$. This implies in particular that γ is surjective. Then P_0 is finitely generated, because P_1 is finitely generated. Indeed, if $(w_1, \ldots, w_n)$ generates P_1, then $(\gamma(w_1), \ldots, \gamma(w_n))$ generates P_0.

(2) First of all, notice that such g_0 and g_2 exist and are indeed unique. For g_0, we have that $\alpha_{|P_0} : P_0 \to \mathrm{Im}(\alpha)$ is an isomorphism of A-modules, because α is injective. So, since $g(\mathrm{Im}(\alpha)) \subseteq \mathrm{Im}(\alpha)$, we can define $g_0 = (\alpha_{|P_0})^{-1} \circ g \circ \alpha_{|P_0}$, which is A-linear because it is a composition of A-linear maps. Then we have that $\alpha \circ g_0 = g \circ \alpha$ and this is the unique definition of g_0 which works. For g_2, notice that, since the sequence is exact, we have $\mathrm{Im}(\alpha) = \mathrm{Ker}(\beta)$. So $g(\mathrm{Ker}(\beta)) \subseteq \mathrm{Ker}(\beta)$. Let $\pi : P_1 \to P_1/\mathrm{Ker}(\beta)$ be the canonical projection. Then we have that $\mathrm{Ker}(\beta) \subseteq \mathrm{Ker}(\pi \circ g)$, so by the universal property of the quotient there is a unique A-linear map $\widetilde{g} : P_1/\mathrm{Ker}(\beta) \to P_1/\mathrm{Ker}(\beta)$ such that $\widetilde{g} \circ \pi = \pi \circ g$. Since β is surjective, by the isomorphism theorem we have an isomorphism of A-modules $\widetilde{\beta} : P_1/\mathrm{Ker}(\beta) \to P_2$ such that $\widetilde{\beta} \circ \pi = \beta$. Then $g_2 = \widetilde{\beta} \circ \widetilde{g} \circ \widetilde{\beta}^{-1}$ is the unique A-linear map $P_2 \to P_2$ such that $g_2 \circ \beta = \beta \circ g$. Let $p_0 : P_0 \oplus P_2 \to P_0$ and $p_2 : P_0 \oplus P_2 \to P_2$ be the canonical projections and define also $i_0 : P_0 \to P_0 \oplus P_2,\ x \mapsto (x, 0)$ and $i_2 : P_2 \to P_0 \oplus P_2,\ y \mapsto (0, y)$. Notice that $p_0 \circ i_0 = \mathrm{id}_{P_0}$, $p_2 \circ i_2 = \mathrm{id}_{P_2}$ and $i_0 \circ p_0 + i_2 \circ p_2 = \mathrm{id}_{P_0 \oplus P_2}$. As in the proof of point (1), we have that the sequence $0 \to P_0 \xrightarrow{\alpha} P_1 \xrightarrow{\beta} P_2 \to 0$ splits. Then there exists an isomorphism $\psi : P_1 \to P_0 \oplus P_2$ such that $\psi \circ \alpha = i_0$ and $\beta \circ \psi^{-1} = p_2$. Define $\gamma := p_0 \circ \psi : P_1 \to P_0$ and $\delta := \psi^{-1} \circ i_2 : P_2 \to P_1$. Then we have that $\gamma \circ \alpha = p_0 \circ \psi \circ \alpha = p_0 \circ i_0 = \mathrm{id}_{P_0}$ and $\beta \circ \delta = \beta \circ \psi^{-1} \circ i_2 = p_2 \circ i_2 = \mathrm{id}_{P_2}$ (see also the proof of lemma 2.1.13). By definition of g_0, we have that

$$g \circ \alpha = \alpha \circ g_0 = \alpha \circ \mathrm{id}_{P_0} \circ g_0 = \alpha \circ \gamma \circ \alpha \circ g_0 = \alpha \circ \gamma \circ g \circ \alpha .$$

By uniqueness, this implies that $g_0 = \gamma \circ g \circ \alpha$. On the other hand, by definition of g_2 we have that

$$\beta \circ g = g_2 \circ \beta = g_2 \circ \mathrm{id}_{P_2} \circ \beta = g_2 \circ \beta \circ \delta \circ \beta = \beta \circ g \circ \delta \circ \beta \ .$$

By uniqueness, this implies that $g_2 = \beta \circ g \circ \delta$.
Let now $\vartheta_{P_0,P_0} : P_0^* \otimes_A P_0 \to \mathrm{End}_A(P_0)$, $\vartheta_{P_1,P_1} : P_1^* \otimes_A P_1 \to \mathrm{End}_A(P_1)$ and $\vartheta_{P_2,P_2} : P_2^* \otimes_A P_2 \to \mathrm{End}_A(P_2)$ be defined as in lemma 2.1.43. They are isomorphisms by corollary 2.1.45. Consider $\vartheta_{P_1,P_1}^{-1}(g) \in P_1^* \otimes P_1$. By definition of tensor product, there exist $n \in \mathbb{N}$, $\varphi_1, \ldots, \varphi_n \in P_1^*$, $p_1, \ldots, p_n \in P$ such that $\vartheta_{P_1,P_1}^{-1}(g) = \varphi_1 \otimes p_1 + \cdots + \varphi_n \otimes p_n$. Applying the definition of ϑ_{P_1,P_1} and the linearity of γ, we get that, for any $x \in P_0$,

$$\begin{aligned} g_0(x) = \gamma(g(\alpha(x))) = \gamma((\vartheta_{P_1,P_1}^{-1}(\varphi_1 \otimes p_1 + \cdots + \varphi_n \otimes p_n))(\alpha(x))) = \\ = \gamma(\varphi_1(\alpha(x))p_1 + \cdots + \varphi_n(\alpha(x))p_n) = \varphi_1(\alpha(x))\gamma(p_1) + \cdots + \varphi_n(\alpha(x))\gamma(p_n) \ . \end{aligned}$$

By definition of ϑ_{P_0,P_0}, this means that $g_0 = \vartheta_{P_0,P_0}((\varphi_1 \circ \alpha) \otimes (\gamma(p_1)) + \cdots + (\varphi_n \circ \alpha) \otimes (\gamma(p_n)))$ (notice that $\varphi_i \circ \alpha \in P_0^*$ and $\gamma(p_i) \in P_0$ for any $i = 1, \ldots, n$). Similarly, for any $x \in P_2$ we have that

$$\begin{aligned} g_2(x) = \beta(g(\alpha(x))) = \beta((\vartheta_{P_1,P_1}^{-1}(\varphi_1 \otimes p_1 + \cdots + \varphi_n \otimes p_n))(\delta(x))) = \\ = \beta(\varphi_1(\delta(x))p_1 + \cdots + \varphi_n(\delta(x))p_n) = \varphi_1(\delta(x))\beta(p_1) + \cdots + \varphi_n(\delta(x))\beta(p_n) \ . \end{aligned}$$

By definition of ϑ_{P_2,P_2}, this means that $g_2 = \vartheta_{P_2,P_2}((\varphi_1 \circ \delta) \otimes (\beta(p_1)) + \cdots + (\varphi_n \circ \delta) \otimes (\beta(p_n)))$ (notice that $\varphi_i \circ \delta \in P_0^*$ and $\beta(p_i) \in P_0$ for any $i = 1, \ldots, n$). Finally, let $\alpha_{P_0} : P_0^* \otimes_A P_0 \to A$, $\alpha_{P_1} : P_1^* \otimes_A P_1 \to A$ and $\alpha_{P_2} : P_2^* \otimes_A P_2 \to A$ be defined as in lemma 2.1.46. Notice that

$$\begin{aligned} \alpha \circ \gamma + \delta \circ \beta = \psi^{-1} \circ i_0 \circ p_0 \circ \psi + \psi^{-1} \circ i_2 \circ p_2 \circ \psi = \\ = \psi^{-1} \circ (i_0 \circ p_0 + i_2 \circ p_2) \circ \psi = \psi^{-1} \circ \mathrm{id}_{P_0 \oplus P_2} \circ \psi = \mathrm{id}_{P_1} \ . \end{aligned}$$

Then, by definition of trace, we have that

$$\begin{aligned} \mathrm{Tr}_{P_0/A}(g_0) + \mathrm{Tr}_{P_2/A}(g_1) = \alpha_{P_0}(\vartheta_{P_0,P_0}^{-1}(g_0)) + \alpha_{P_2}(\vartheta_{P_2,P_2}^{-1}(g_0)) = \\ = \alpha_{P_0}\left(\sum_{i=1}^{n}(\varphi_i \circ \alpha) \otimes (\gamma(p_i))\right) + \alpha_{P_2}\left(\sum_{i=1}^{n}(\varphi_i \circ \delta) \otimes (\beta(p_i))\right) = \\ = \sum_{i=1}^{n}(\varphi_i \circ \alpha)(\gamma(p_i)) + \sum_{i=1}^{n}(\varphi_i \circ \delta)(\beta(p_i)) = \\ = \sum_{i=1}^{n}(\varphi_i((\alpha \circ \gamma)(p_i)) + \varphi_i((\delta \circ \beta)(p_i))) = \sum_{i=1}^{n}(\varphi_i((\alpha \circ \gamma + \delta \circ \beta)(p_i))) = \\ = \sum_{i=1}^{n}\varphi_i(p_i) = \alpha_{P_1}\left(\sum_{i=1}^{n}\varphi_i \otimes p_i\right) = \alpha_{P_1}(\vartheta_{P_1,P_1}^{-1}(g)) = \mathrm{Tr}_{P_1/A}(g) \ , \end{aligned}$$

as we wanted.

□

Corollary 2.1.63. *Let $B_1, \dots, B_n$ be finite projective A-algebras and define $B := \prod_{i=1}^n B_i$ (which is also a finite projective A-algebra, by lemma 2.1.52). For every $b_1 \in B_1, \dots, b_n \in B_n$, we have that*

$$\mathrm{Tr}_{B/A}((b_1, \dots, b_n)) = \sum_{i=1}^n \mathrm{Tr}_{B_i/A}(b_i) \ .$$

Proof. We prove the claim in the case $n = 2$. Then the general case follows by induction.
We have that $B = B_1 \times B_2$, as an A-module, coincides with $B_1 \oplus B_2$. Consider the A-linear maps $i_1 : B_1 \to B,\ x \mapsto (x, 0)$ and $p_2 : B \to B_2,\ (x_1, x_2) \mapsto x_2$ and the short exact sequence

$$0 \to B_1 \xrightarrow{i_1} B \xrightarrow{p_2} B_2 \to 0 \ .$$

Let $b_1 \in B_1$, $b_2 \in B_2$. For every $x_1 \in B_1$, $x_2 \in B_2$, we have that

$$m_{(b_1,b_2)}((x_1, x_2)) = (b_1, b_2) \cdot (x_1, x_2) = (b_1 x_1, b_2 x_2) = (m_{b_1}(x_1), m_{b_2}(x_2)) \ .$$

Then, for every $x \in B_1$, we have that

$$m_{(b_1,b_2)}(i_1(x)) = m_{(b_1,b_2)}((x, 0)) = (m_{b_1}(x), m_{b_2}(0)) = (m_{b_1}(x), 0) = i_1(m_{b_1}(x)) \ .$$

So $m_{(b_1,b_2)}(\mathrm{Im}(i_1)) \subseteq \mathrm{Im}(i_1)$ and that $m_{(b_1,b_2)} \circ i_1 = i_1 \circ m_{b_1}$. Moreover, for every $x_1 \in B_1$, $x_2 \in B_2$, we have that $p_2(m_{(b_1,b_2)}((x_1, x_2))) = p_2((m_{b_1}(x_1), m_{b_2}(x_2))) = m_{b_2}(x_2) = m_{b_2}(p_2((x_1, x_2)))$. So $p_2 \circ m_{b_1,b_2} = m_{b_2} \circ p_2$. Hence, by lemma 2.1.62, we have that

$$\begin{aligned} \mathrm{Tr}_{B/A}((b_1, b_2)) = \mathrm{Tr}_{B/A}(m_{(b_1,b_2)}) = \\ = \mathrm{Tr}_{B_1/A}(m_{b_1}) + \mathrm{Tr}_{B_2/A}(m_{b_2}) = \mathrm{Tr}_{B_1/A}(b_1) + \mathrm{Tr}_{B_2/A}(b_2) \ , \end{aligned}$$

as we wanted. □

Lemma 2.1.64. *Let $B_1, \dots, B_n$ be A-algebras and define $B := \prod_{i=1}^n B_i$. Then B is a projective separable A-algebra if and only if B_i is a projective separable A-algebra for every $i = 1, \dots, n$.*

Proof. By lemma 2.1.52, we know that B is finite projective if and only if B_i is finite projective for every $i = 1, \dots, n$. Assume that this holds and let $\varphi : B \to \mathrm{Hom}_A(B, A)$ be the map defined in lemma 2.1.59. Moreover, for any $i \in I$, let $\varphi_i : B_i \to \mathrm{Hom}_A(B_i, A)$ be the map defined in the same way, but considering B_i instead of B. We have to prove that φ is bijective if and only if φ_i is bijective for every $i = 1, \dots, n$. Recall that, as an A-module, $B = \prod_{i=1}^n B_i$ coincides with $\bigoplus_{i=1}^n B_i$. Then, by lemma 2.1.9, we have an isomorphism of A-modules $\varphi_A : \mathrm{Hom}_A(B, A) \to \prod_{i=1}^n \mathrm{Hom}_A(B_i, A)$. Define

$$\psi : B \to \prod_{i=1}^n \mathrm{Hom}_A(B_i, A),\ (b_1, \dots, b_n) \mapsto (\varphi_1(b_1), \dots, \varphi_n(b_n))$$

and consider the following diagram.

$$\begin{array}{ccc} B & \xrightarrow{\varphi} & \mathrm{Hom}_A(B,A) \\ & \searrow^{\psi} & \downarrow{\scriptstyle \varphi_A} \\ & & \prod_{i=1}^n \mathrm{Hom}_A(B_i,A) \end{array}$$

Let $(b_1,\dots,b_n) \in B$. Fix $j \in \{1,\dots,n\}$ and consider the A-linear map $q_j : B_j \to B$, $x \mapsto (\delta_{ij}x)_{i=1,\dots,n}$. Let $x \in B_j$. Applying corollary 2.1.63, we have that

$$\begin{aligned}(\varphi((b_1,\dots,b_n)) \circ q_j)(x) &= \varphi((b_1,\dots,b_n))((\delta_{ij}x)_{i=1,\dots,n}) = \\ &= \mathrm{Tr}_{B/A}((b_1,\dots,b_n)\cdot(\delta_{ij}x)_{i=1,\dots,n}) = \mathrm{Tr}_{B/A}((b_i\delta_{ij}x)_{i=1,\dots,n}) = \\ &= \sum_{i=1}^n \mathrm{Tr}_{B_i/A}(b_i\delta_{ij}x) = \mathrm{Tr}_{B_j/A}(b_jx) = \varphi_j(b_j)(x)\end{aligned}$$

(recall that $\mathrm{Tr}_{B_i/A}(0) = 0$ for any $i = 1,\dots,n$, by linearity of the trace: see remark 2.1.48). Then $\varphi((b_1,\dots,b_n)) \circ q_j = \varphi_j(b_j)$. Since this holds for any $j = 1,\dots,n$, we get that

$$\begin{aligned}\varphi_A(\varphi((b_1,\dots,b_n))) &= (\varphi((b_1,\dots,b_n)) \circ q_1,\dots,\varphi((b_1,\dots,b_n)) \circ q_n) = \\ &= (\varphi_1(b_1),\dots,\varphi_n(b_n)) = \psi((b_1,\dots,b_n)) \ .\end{aligned}$$

So $\varphi_A \circ \varphi = \psi$. Since φ_A is bijective, it follows that φ is bijective if and only if ψ is bijective. But we have that

$$\begin{aligned}&\mathrm{Ker}(\psi) = \\ &= \{(b_1,\dots,b_n) \in B \mid (\varphi_1(b_1),\dots,\varphi_n(b_n)) = \psi((b_1,\dots,b_n)) = (0,\dots,0)\} = \\ &\{(b_1,\dots,b_n) \in B \mid \forall i = 1,\dots,n \quad \varphi_i(b_i) = 0\} = \prod_{i=1}^n \mathrm{Ker}(\varphi_i)\end{aligned}$$

and

$$\begin{aligned}\mathrm{Im}(\psi) &= \left\{(f_1,\dots,f_n) \in \prod_{i=1}^n \mathrm{Hom}_A(B_i,A) \;\middle|\; \exists (b_1,\dots,b_n) \in B : \right. \\ &\left. (\varphi_1(b_1),\dots,\varphi_n(b_n)) = \psi((b_1,\dots,b_n)) = (f_1,\dots,f_n)\right\} = \\ &= \left\{(f_1,\dots,f_n) \in \prod_{i=1}^n \mathrm{Hom}_A(B_i,A) \;\middle|\; \forall i = 1,\dots,n \ \exists b_i \in B_i : \varphi_i(b_i) = f_i\right\} = \\ &= \prod_{i=1}^n \mathrm{Im}(\varphi_i) \ .\end{aligned}$$

Then $\mathrm{Ker}(\psi) = 0$ if and only if $\mathrm{Ker}(\varphi_i) = 0$ for every $i = 1,\dots,n$, i.e. ψ is injective if and only if φ_i is injective for every $i = 1,\dots,n$, and $\mathrm{Im}(\psi) = \prod_{i=1}^n \mathrm{Hom}_A(B_i,A)$ if and only if $\mathrm{Im}(\varphi_i) = \mathrm{Hom}_A(B_i,A)$ for every $i = 1,\dots,n$, i.e. ψ is surjective if and only if φ_i is surjective for every $i = 1, \dots, n$. So ψ is bijective if and only if φ_i is bijective for every $i = 1, \dots, n$, and hence φ is bijective if and only if φ_i is bijective for every $i = 1, \dots, n$, which is what we wanted. □

Lemma 2.1.65. *Let B be an A-algebra. For any B-module P (including B itself), consider $\mathrm{Hom}_A(P, A)$ as a B-module via $(bf)(x) = f(bx)$ for any $b \in B$, $f \in \mathrm{Hom}_A(P, A)$ and $x \in P$ (recall that we have an induced A-module structure on P, so it makes sense to consider $\mathrm{Hom}_A(P, A)$). Then, for any B-module P, we have a B-linear map*

$$\gamma_P : \mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(P, B) \to \mathrm{Hom}_A(P, A),\ f \otimes g \mapsto f \otimes g$$

(extended by linearity). If $P = \bigoplus_{i=1}^n P_i$ for some B-modules $P_1, \dots, P_n$, then γ_P is bijective if and only if γ_{P_i} is bijective for every $i = 1, \dots, n$.

Proof. Let P be a B-module. First of all, we prove that the definition we gave makes indeed $\mathrm{Hom}_A(P, A)$ into a B-module. Let $b \in B$, $f \in \mathrm{Hom}_A(P, A)$. For any $a_1, a_2 \in A$, $x_1, x_2 \in P$ we have that

$$\begin{aligned}(bf)(a_1x_1 + a_2x_2) &= f(b(a_1x_1 + a_2x_2)) = \\ &= f(b(a_1x_1) + b(a_2x_2)) = f((a_1b)x_1 + (a_2b)x_2) = \\ &= f(a_1(bx_1) + a_2(bx_2)) = a_1f(bx_1) + a_2f(bx_2) = a_1(bf)(x_1) + a_2(bf)(x_2)\ .\end{aligned}$$

So bf is A-linear, i.e. $bf \in \mathrm{Hom}_A(P, A)$.
For any $f \in \mathrm{Hom}_A(P, A)$, we have that $(1_Bf)(x) = f(1_Bx) = f(x)$ for any $x \in P$ and so $1_Bf = f$. Let now $b_1, b_2 \in B$ and $f \in \mathrm{Hom}_A(P, A)$. For every $x \in P$, we have that

$$\begin{aligned}((b_1 + b_2)f)(x) &= f((b_1 + b_2)x) = f(b_1x + b_2x) = \\ &= f(b_1x) + f(b_2x) = (b_1f)(x) + (b_2f)(x) = (b_1f + b_2f)(x)\end{aligned}$$

and

$$((b_1b_2)f)(x) = f((b_1b_2)x) = f((b_2b_1)x) = f(b_2(b_1x)) = (b_2f)(b_1x) = (b_1(b_2f))(x)\ .$$

So $(b_1 + b_2)f = b_1f + b_2f$ and $(b_1b_2)f = b_1(b_2f)$. On the other hand, let $b \in B$ and $f_1, f_2 \in \mathrm{Hom}_A(P, A)$. For any $x \in P$ we have that

$$(b(f_1+f_2))(x) = (f_1+f_2)(bx) = f_1(bx)+f_2(bx) = (bf_1)(x)+(bf_2)(x) = (bf_1+bf_2)(x).$$

So $b(f_1 + f_2) = bf_1 + bf_2$. Then we have a B-module structure on $\mathrm{Hom}_A(P, A)$ for any B-module P. In particular, we have a B-module structure on $\mathrm{Hom}_A(B, A)$. Notice also that the B-module structure we have just defined on $\mathrm{Hom}_A(P, A)$ induces an A-module structure which coincides with the standard A-module structure on $\mathrm{Hom}_A(P, A)$ (this follows immediately from the definition of A-linear map).
Since any B-linear map is also A-linear, for any $f \in \mathrm{Hom}_A(B, A)$, $g \in \mathrm{Hom}_B(P, B)$ we have that $f \circ g \in \mathrm{Hom}_A(P, A)$. In order to show that γ_P is well defined, we have to check that the map $\Gamma_P : \mathrm{Hom}_A(B, A) \times \mathrm{Hom}_B(P, B) \to \mathrm{Hom}_A(P, A)$, $(f, g) \mapsto f \circ g$

is B-bilinear. Let $b_1, b_2 \in B$, $f_1, f_2 \in \mathrm{Hom}_A(B, A)$ and $g \in \mathrm{Hom}_B(P, B)$. For any $x \in P$, we have that

$$\begin{aligned}((b_1 f_1 + b_2 f_2) \circ g)(x) &= (b_1 f_1)(g(x)) + (b_2 f_2)(g(x)) = \\ &= f_1(b_1 g(x)) + f_2(b_2 g(x)) = f_1(g(b_1 x)) + f_2(g(b_2 x)) = \\ &= (b_1(f_1 \circ g))(x) + (b_2(f_2 \circ g))(x) = (b_1(f_1 \circ g) + b_2(f_2 \circ g))(x) \ .\end{aligned}$$

So $\Gamma_P((b_1 f_1 + b_2 f_2, g)) = (b_1 f_1 + b_2 f_2) \circ g = b_1(f_1 \circ g) + b_2(f_2 \circ g) = b_1 \Gamma_P((f_1, g)) + b_2 \Gamma_P((f_2, g))$. On the other hand, let $b_1, b_2 \in B$, $f \in \mathrm{Hom}_A(B, A)$ and $g_1, g_2 \in \mathrm{Hom}_B(P, B)$. For any $x \in P$, we have that

$$\begin{aligned}(f \circ (b_1 g_1 + b_2 g_2))(x) &= f(b_1 g_1(x) + b_2 g_2(x)) = \\ &= f(b_1 g_1(x)) + f(b_2 g_2(x)) = f(g_1(b_1 x)) + f(g_2(b_2 x)) = \\ &= (b_1(f \circ g_1))(x) + (b_2(f \circ g_2))(x) = (b_1(f \circ g_1) + b_2(f \circ g_2))(x) \ .\end{aligned}$$

So $\Gamma_P((f, b_1 g_2 + b_2 g_2)) = f \circ (b_1 g_1 + b_2 g_2) = b_1(f \circ g_1) + b_2(f \circ g_2) = b_1 \Gamma_P((f, g_1)) + b_2 \Gamma_P((f, g_2))$. This proves that Γ_P is B-bilinear. So γ_P is well defined.
Assume now that $P = \bigoplus_{i=1}^n P_i$, for some B-modules $P_1, \ldots, P_n$. For any $j = 1, \ldots, n$, define $q_j : P_j \to P$, $x \mapsto (\delta_{ij} x)_{i=1,\ldots,n}$ (then q_j is B-linear). As in lemma 2.1.9, consider the isomorphisms $\varphi_A : \mathrm{Hom}_A(P, A) \to \prod_{i=1}^n \mathrm{Hom}_A(P_i, A)$ and $\varphi_B : \mathrm{Hom}_B(P, B) \to \prod_{i=1}^n \mathrm{Hom}_B(P_i, B)$, of A-modules and of B-modules respectively (for the latter isomorphism, we apply the lemma with B instead of A). Notice that φ_A is also B-linear. Indeed, if $b \in B$, $f \in \mathrm{Hom}_A(P, A)$ and $i \in \{1, \ldots, n\}$, we have that $((bf) \circ q_i)(x) = (bf)(q_i(x)) = f(b q_i(x)) = f(q_i(bx)) = (b(f \circ q_i))(x)$, for any $x \in P_i$. So $(bf) \circ q_i = b(f \circ q_i)$, for any $i = 1, \ldots, n$, and

$$\varphi_A(bf) = ((bf) \circ q_i)_{i=1,\ldots,n} = (b(f \circ q_i))_{i=1,\ldots,n} = b(f \circ q_i)_{i=1,\ldots,n} = b\vartheta_A(f) \ .$$

Notice also that, since the direct sum of a *finite* family of modules coincides with its direct product, $\prod_{i=1}^n \mathrm{Hom}_A(P_i, A) = \bigoplus_{i=1}^n \mathrm{Hom}_A(P_i, A)$ and $\prod_{i=1}^n \mathrm{Hom}_B(P_i, B) = \bigoplus_{i=1}^n \mathrm{Hom}_B(P_i, B)$. Consider the isomorphism of B-modules $\mathrm{id}_{\mathrm{Hom}_A(B,A)} \otimes \varphi_B : \mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(P, B) \to \mathrm{Hom}_A(B, A) \otimes_B \bigoplus_{i=1}^n \mathrm{Hom}_B(P_i, B)$ induced by φ_B. Moreover, consider the isomorphism of B-modules $\psi_{\mathrm{Hom}_A(B,A)} : \mathrm{Hom}_A(B, A) \otimes_B \bigoplus_{i=1}^n \mathrm{Hom}_B(P_i, B) \to \bigoplus_{i=1}^n (\mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(P_i, B))$ as in lemma 2.1.19 (actually here we have the direct sum on the other factor, but by commutativity of the tensor product this is not a problem). Then we have the following diagram.

$$\begin{array}{ccc} \mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(P, B) & \xrightarrow{\gamma_P} & \mathrm{Hom}_A(P, A) \\ \Big\downarrow \psi_{\mathrm{Hom}_A(B,A)} \circ (\mathrm{id}_{\mathrm{Hom}_A(B,A)} \otimes \varphi_B) & & \Big\downarrow \varphi_A \\ \bigoplus_{i=1}^n (\mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(P_i, B)) & \xrightarrow{\bigoplus_{i=1}^n \gamma_{P_i}} & \bigoplus_{i=1}^n \mathrm{Hom}_A(P_i, A) \end{array}$$

We claim that this diagram is commutative. Let $f \in \mathrm{Hom}_A(B, A)$, $g \in \mathrm{Hom}_B(P, B)$. We have that

$$\varphi_A(\gamma_P(f \otimes g)) = \varphi_A(f \circ g) = (f \circ g \circ q_i)_{i=1,\ldots,n} = (\gamma_{P_i}(f \otimes (g \circ q_i)))_{i=1,\ldots,n} =$$

$$= \left(\bigoplus_{i=1}^{n} \gamma_{P_i}\right) ((f \otimes (g \circ q_i))_{i=1,\dots,n}) =$$

$$= \left(\bigoplus_{i=1}^{n} \gamma_{P_i}\right) \left(\psi_{\mathrm{Hom}_A(B,A)}\left(f \otimes (g \circ q_i)_{i=1,\dots,n}\right)\right) =$$

$$= \left(\left(\bigoplus_{i=1}^{n} \gamma_{P_i}\right) \circ \psi_{\mathrm{Hom}_A(B,A)}\right) \left((\mathrm{id}_{\mathrm{Hom}_A(B,A)} \otimes \varphi_B)(f \otimes g)\right) .$$

Then $\varphi_A \circ \gamma_P = (\bigoplus_{i=1}^n \gamma_{P_i}) \circ (\psi_{\mathrm{Hom}_A(B,A)} \circ (\mathrm{id}_{\mathrm{Hom}_A(B,A)} \otimes \varphi_B))$ (since we are dealing with B-linear maps, it is enough to check equality on pure tensors), i.e. the diagram is commutative. Since φ_A and $\psi_{\mathrm{Hom}_A(B,A)} \circ (\mathrm{id}_{\mathrm{Hom}_A(B,A)} \otimes \varphi_B)$ are isomorphisms, it follows that γ_P is bijective if and only if $\bigoplus_{i=1}^n \gamma_{P_i}$ is bijective. It is easy to prove that

$$\mathrm{Ker}\left(\bigoplus_{i=1}^{n} \gamma_{P_i}\right) = \bigoplus_{i=1}^{n} \mathrm{Ker}(\gamma_{P_i})$$

and

$$\mathrm{Im}\left(\bigoplus_{i=1}^{n} \gamma_{P_i}\right) = \bigoplus_{i=1}^{n} \mathrm{Im}(\gamma_{P_i})$$

(see the proof of corollary 2.1.20). So $\mathrm{Ker}\,(\bigoplus_{i=1}^n \gamma_{P_i}) = 0$ if and only if $\mathrm{Ker}(\gamma_{P_i}) = 0$ for any $i = 1, \dots, n$, i.e. $\bigoplus_{i=1}^n \gamma_{P_i}$ is injective if and only if γ_{P_i} is injective for any $i = 1, \dots, n$, and $\mathrm{Im}\,(\bigoplus_{i=1}^n \gamma_{P_i}) = \bigoplus_{i=1}^n \mathrm{Hom}_A(P_i, A)$ if and only if $\mathrm{Im}(\gamma_{P_i}) = \mathrm{Hom}_A(P_i, A)$ for any $i = 1, \dots, n$, i.e. $\bigoplus_{i=1}^n \gamma_{P_i}$ is surjective if and only if γ_{P_i} is surjective for any $i = 1, \dots, n$. Hence $\bigoplus_{i=1}^n \gamma_{P_i}$ is bijective if and only if γ_{P_i} is bijective for every $i = 1, \dots, n$, which ends the proof. □

Corollary 2.1.66. *Let B be an A-algebra and P a finitely generated and projective B-module. Then the map $\gamma_P : \mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(P, B) \to \mathrm{Hom}_A(P, A)$ defined as in lemma 2.1.65 is bijective.*

Proof. Since P is finitely generated and projective as a B-module, by corollary 2.1.15 there exist a B-module Q and an $n \in \mathbb{N}$ such that $P \oplus Q \cong B^n$ as B-modules. By lemma 2.1.65, in order to prove that γ_P is bijective, it is enough to show that γ_{B^n} is bijective. By the same lemma, in order to prove that γ_{B^n} is bijective, it is enough to prove that γ_B is bijective. We have that $\mathrm{Hom}_B(B, B) \cong B$ as B-modules, via $\varphi : \mathrm{Hom}_B(B, B) \to B$, $f \mapsto f(1_B)$. Then $\mathrm{id}_{\mathrm{Hom}_A(B,A)} \otimes \varphi : \mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(B, B) \to \mathrm{Hom}_A(B, A) \otimes_B B$ is an isomorphism of B-modules. Moreover, $\mathrm{Hom}_A(B, A) \otimes_B B \cong \mathrm{Hom}_A(B, A)$ as B-modules, via $\psi : \mathrm{Hom}_A(B, A) \otimes_B B \to \mathrm{Hom}_A(B, A)$, $f \otimes b \mapsto bf$. For any $f \in \mathrm{Hom}_A(B, A)$, $g \in \mathrm{Hom}_B(B, B)$, we have that

$$\psi((\mathrm{id}_{\mathrm{Hom}_A(B,A)} \otimes \varphi)(f \otimes g)) = \psi(f \otimes \varphi(g)) = \psi(f \otimes g(1_B)) = g(1_B)f .$$

For any $x \in B$, $(g(1_B)f)(x) = f(g(1_B)x) = f(g(1_B x)) = f(g(x))$. So

$$\psi((\mathrm{id}_{\mathrm{Hom}_A(B,A)} \otimes \varphi)(f \otimes g)) = g(1_B)f = f \circ g = \gamma_B(f \otimes g) .$$

Then $\gamma_B = \psi \circ (\mathrm{id}_{\mathrm{Hom}_A(B,A)} \otimes \varphi)$ (since we are dealing with B-linear maps, it is enough to check equality on pure tensors). So γ_B is bijective, because it is a composition of bijections. This ends the proof. □

Remark 2.1.67. In the proof of lemma 2.1.65, a key point was the fact that we were dealing with a *finite* direct sum. Then also in corollary 2.1.66 it was important to assume that P was finitely generated over B.

Lemma 2.1.68. *Let B be a finite projective A-algebra and P a finitely generated and projective B-module. For any $\varphi \in \mathrm{End}_B(P)$, we have that* $\mathrm{Tr}_{P/A}(\varphi) = \mathrm{Tr}_{B/A}(\mathrm{Tr}_{P/B}(\varphi))$.

Proof. First of all, notice that P is finitely generated and projective over A by lemma 2.1.53 and that, since any B-linear map is also A-linear, $\varphi \in \mathrm{End}_A(P)$. So it makes sense to consider the trace $\mathrm{Tr}_{P/A}(\varphi)$. Moreover, as in lemma 2.1.59, $\mathrm{Tr}_{B/A}(\mathrm{Tr}_{P/B}(\varphi)) := \mathrm{Tr}_{B/A}(m_{\mathrm{Tr}_{P/B}(\varphi)})$.
Since P is finitely generated and projective over B, by lemma 2.1.49(1) (with B instead of A) there exist $n \in \mathbb{N}$, $x_1, \ldots, x_n \in P$ and $f_1, \ldots, f_n \in \mathrm{Hom}_B(P, B)$ such that, for every $x \in P$, we have $x = \sum_{i=1}^{n} f_i(x)x_i$. By the same lemma, since B is a finite projective A-algebra, i.e. it is finitely generated and projective as an A-module, there exist $m \in \mathbb{N}$, $b_1, \ldots, b_m \in B$ and $g_1, \ldots, g_m \in \mathrm{Hom}_A(B, A)$ such that, for every $b \in B$, we have $b = \sum_{j=1}^{m} g_j(b)b_j$. For every $i = 1, \ldots, n$, $j = 1, \ldots, m$, consider $b_j x_i \in P$ and $g_j \circ f_i \in \mathrm{Hom}_A(P, A)$ (notice that this works because any B-linear map is also A-linear). For every $x \in P$, we have that

$$x = \sum_{i=1}^{n} f_i(x)x_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} g_j(f_i(x))b_j \right) x_i = \sum_{i=1}^{n} \sum_{j=1}^{m} (g_j \circ f_i)(x)(b_j x_i) .$$

Then, by lemma 2.1.49(2), we have that

$$\begin{aligned}
\mathrm{Tr}_{P/A}(\varphi) &= \sum_{i=1}^{n} \sum_{j=1}^{m} (g_j \circ f_i)(\varphi(b_j x_i)) = \sum_{i=1}^{n} \sum_{j=1}^{m} g_j(f_i(b_j \varphi(x_i))) = \\
&= \sum_{j=1}^{m} \sum_{i=1}^{n} g_j(b_j f_i(\varphi(x_i))) = \sum_{j=1}^{m} g_j \left(\sum_{i=1}^{n} b_j f_i(\varphi(x_i)) \right) = \\
&= \sum_{j=1}^{m} g_j \left(b_j \sum_{i=1}^{n} f_i(\varphi(x_i)) \right) = \sum_{j=1}^{m} g_j(b_j \, \mathrm{Tr}_{C/B}(\varphi)) = \\
&= \sum_{j=1}^{m} g_j(m_{\mathrm{Tr}_{C/B}(\varphi)}(b_j)) = \mathrm{Tr}_{B/A}(m_{\mathrm{Tr}_{C/B}(\varphi)}) = \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(\varphi)) .
\end{aligned}$$

□

Corollary 2.1.69. *Let B be a projective separable A-algebra and C a projective separable B-algebra. Consider the induced A-algebra structure on C. Then C is a projective separable A-algebra.*

Proof. Since B is a projective separable A-algebra, it is in particular finite projective. Analogously, C is a finite projective B-algebra. By corollary 2.1.54, we have that C is a finite projective A-algebra. Let $\varphi_B : B \to \mathrm{Hom}_A(B, A)$ be the map defined in lemma 2.1.59 and $\varphi_C : C \to \mathrm{Hom}_A(C, A)$ the map defined in the same way, with C instead of B. Moreover, let $\varphi'_C : C \to \mathrm{Hom}_B(C, B)$ be the map defined as in lemma 2.1.59, with B instead of A and C instead of B. Let $x \in C$. Applying lemma 2.1.68, we have that

$$\varphi_C(x)(y) = \mathrm{Tr}_{C/A}(xy) = \mathrm{Tr}_{C/A}(m_{xy}) = \\ = \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(m_{xy})) = \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(xy)) = \mathrm{Tr}_{B/A}(\varphi'_C(x)(y))$$

for any $y \in C$. So $\varphi_C(x) = \mathrm{Tr}_{B/A} \circ (\varphi'_C(x))$. Define

$$(\mathrm{Tr}_{B/A})_* : \mathrm{Hom}_B(C, B) \to \mathrm{Hom}_A(C, A),\ f \mapsto \mathrm{Tr}_{B/A} \circ f$$

(this is well defined because any B-linear map from C to B is also A-linear and $\mathrm{Tr}_{B/A} : B \to A$ is A-linear by 2.1.59). Then $\varphi_C(x) = (\mathrm{Tr}_{B/A})_*(\varphi'_C(x))$. Since this holds for any $x \in C$, we have that $\varphi_C = (\mathrm{Tr}_{B/A})_* \circ \varphi'_C$. We have that φ'_C is bijective, because C is a projective separable B-algebra. Since B is a projective separable A-algebra, we have that $\varphi_B : B \to \mathrm{Hom}_A(B, A)$ is an isomorphism of A-modules. Moreover, if we consider on $\mathrm{Hom}_A(B, A)$ the B-module structure defined in lemma 2.1.65, we have that φ_B is also B-linear. Indeed, if $b, x \in B$ we have that $\varphi_B(bx)(y) = \mathrm{Tr}_{B/A}((bx)y) = \mathrm{Tr}_{B/A}(x(by)) = \varphi_B(x)(by) = (b\varphi_B(x))(y)$ for any $y \in B$ and so $\varphi_B(bx) = b\varphi_B(x)$. Then φ_B induces an isomorphism of B-modules

$$\varphi_B \otimes \mathrm{id}_{\mathrm{Hom}_B(C,B)} : B \otimes_B \mathrm{Hom}_B(C, B) \to \mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(C, B) .$$

We have that $B \otimes_B \mathrm{Hom}_B(C, B) \cong \mathrm{Hom}_B(C, B)$ as B-modules, via $\psi : B \otimes_B \mathrm{Hom}_B(C, B) \to \mathrm{Hom}_B(C, B),\ b \otimes f \mapsto bf$, which has inverse $\psi^{-1} : \mathrm{Hom}_B(C, B) \to B \otimes_B \mathrm{Hom}_B(C, B),\ f \mapsto 1_B \otimes f$. Moreover, let $\gamma_C : \mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(C, B) \to \mathrm{Hom}_A(C, A)$ be as in lemma 2.1.65. By corollary 2.1.66, we have that γ_C is an isomorphism, because C is finitely generated and projective as a B-module. Consider $\gamma_C \circ (\varphi_B \otimes \mathrm{id}_{\mathrm{Hom}_B(C,B)}) \circ \psi^{-1} : \mathrm{Hom}_B(C, B) \to \mathrm{Hom}_A(B, A)$. For any $f \in \mathrm{Hom}_B(C, B)$, we have that

$$(\gamma_C \circ (\varphi_B \otimes \mathrm{id}_{\mathrm{Hom}_B(C,B)}) \circ \psi^{-1})(f) = \gamma_C((\varphi_B \otimes \mathrm{id}_{\mathrm{Hom}_B(C,B)})(\psi^{-1}(f))) = \\ = \gamma_C((\varphi_B \otimes \mathrm{id}_{\mathrm{Hom}_B(C,B)})(1_B \otimes f)) = \gamma_C(\varphi_B(1_B) \otimes f) = \varphi_B(1_B) \circ f .$$

But, for any $y \in B$, we have that $\varphi_B(1_B)(y) = \mathrm{Tr}_{B/A}(1_B y) = \mathrm{Tr}_{B/A}(y)$. So $\varphi_B(1_B) = \mathrm{Tr}_{B/A}$ and $(\gamma_C \circ (\varphi_B \otimes \mathrm{id}_{\mathrm{Hom}_B(C,B)}) \circ \psi^{-1})(f) = \varphi_B(1_B) \circ f = \mathrm{Tr}_{B/A} \circ f = (\mathrm{Tr}_{B/A})_*(f)$. Then $(\mathrm{Tr}_{B/A})_* = \gamma_C \circ (\varphi_B \otimes \mathrm{id}_{\mathrm{Hom}_B(C,B)}) \circ \psi^{-1}$, which implies that $\varphi_C = (\mathrm{Tr}_{B/A})_* \circ \varphi'_C = \gamma_C \circ (\varphi_B \otimes \mathrm{id}_{\mathrm{Hom}_B(C,B)}) \circ \psi^{-1} \circ \varphi'_C$ is bijective, because it is a composition of bijections. Hence C is a projective separable A-algebra. □

Lemma 2.1.70. *Let P be a finitely generated projective A-module and B an A-algebra. For any $f \in \mathrm{End}_A(P)$, we have that* $\mathrm{Tr}_{P \otimes_A B/B}(f \otimes \mathrm{id}_B) = \mathrm{Tr}_{P/A}(f) \cdot 1$.

Proof. First of all, notice that by lemma 2.1.24, $P \otimes_A B$ is a projective B-module. It is also clear that $P \otimes_A B$ is finitely generated as a B-module (see the proof of proposition 2.1.57). So it makes sense to consider the trace $\mathrm{Tr}_{P \otimes_A B/B}$ of a B-linear

map $P \otimes_A B \to P \otimes_A B$. If $f : P \to P$ is A-linear, it is immediate to prove that $f \otimes \mathrm{id}_B : P \otimes_A B \to P \otimes_A B$ is B-linear. So $\mathrm{Tr}_{P\otimes_A B/B}(f \otimes \mathrm{id}_B)$ is well defined.
Let $\vartheta_{P,P} : P^* \otimes_A P \to \mathrm{End}_A(P)$ and $\vartheta_{P\otimes_A B,P\otimes_A B} : (P \otimes_A B)^* \otimes_B (P \otimes_A B) \to \mathrm{End}_B(P \otimes_A B)$ be defined as in lemma 2.1.43. By corollary 2.1.45, they are isomorphisms (respectively, of A-modules and of B-modules). Let also $\alpha_P : P^* \otimes_A P \to A$, $\alpha_{P\otimes_A B} : (P \otimes_A B)^* \otimes_B (P \otimes_A B) \to B$ be defined as in lemma 2.1.46. Since $\vartheta_{P,P}$ is an isomorphism, we have that $\mathrm{End}_A(P)$ is generated by the elements of the form $\vartheta_{P,P}(\varphi \otimes p)$, with $\varphi \in P^*$ and $p \in P$. Notice that $- \otimes \mathrm{id}_B : \mathrm{End}_A(P) \to \mathrm{End}_B(P \otimes_A B)$ is A-linear. Also the trace is A-linear (remark 2.1.48). Then it is enough to prove that the claim is true for $f = \vartheta_{P,P}(\varphi \otimes p)$, with $\varphi \in P^*$ and $p \in P$. In this case, we have that

$$\mathrm{Tr}(f) = \alpha_P(\vartheta_{P,P}^{-1}(f)) = \alpha_P(\varphi \otimes p) = \varphi(p) \; .$$

Moreover, $\varphi \otimes \mathrm{id}_B : P \otimes_A B \to A \otimes_A B$ is a B-linear map and composing it with the canonical isomorphism of B-modules $\psi : A \otimes_A B \to B$, $a \otimes b \mapsto ab$ we get $\psi \circ (\varphi \otimes \mathrm{id}_B) \in (P \otimes_A B)^*$. For any $x \in P$, $y \in B$, we have that

$$\begin{aligned}\vartheta_{P\otimes_A B,P\otimes_A B}((\psi \circ (\varphi \otimes \mathrm{id}_B)) \otimes (p \otimes 1))(x \otimes y) &= (\psi \circ (\varphi \otimes \mathrm{id}_B))(x \otimes y) \cdot (p \otimes 1) = \\ = \psi(\varphi(x) \otimes y) \cdot (p \otimes 1) &= (\varphi(x)y) \cdot (p \otimes 1) = (\varphi(x)p) \otimes y = \\ &= (\vartheta_{P,P}(\varphi \otimes p)(x)) \otimes y = f(x) \otimes y = (f \otimes \mathrm{id}_B)(x \otimes y) \; .\end{aligned}$$

So $\vartheta_{P\otimes_A B,P\otimes_A B}((\psi\circ(\varphi\otimes\mathrm{id}_B))\otimes(p\otimes 1))) = f\otimes\mathrm{id}_B$ (by linearity, it is enough to check equality on pure tensors). Then $\vartheta^{-1}_{P\otimes_A B,P\otimes_A B}(f \otimes \mathrm{id}_B) = (\psi \circ (\varphi \otimes \mathrm{id}_B)) \otimes (p \otimes 1)$ and

$$\begin{aligned}\mathrm{Tr}_{P\otimes_A B,B}(f \otimes \mathrm{id}_B) &= \alpha_{P\otimes_A B}(\vartheta^{-1}_{P\otimes_A B,P\otimes_A B}(f \otimes \mathrm{id}_B)) = \\ &= \alpha_{P\otimes_A B}((\psi \circ (\varphi \otimes \mathrm{id}_B)) \otimes (p \otimes 1)) = (\psi \circ (\varphi \otimes \mathrm{id}_B))(p \otimes 1) = \\ &= \psi(\varphi(p) \otimes 1) = \varphi(p) \cdot 1 = \mathrm{Tr}_{P/A}(f) \cdot 1 \; ,\end{aligned}$$

as we wanted. □

Lemma 2.1.71. *Let B and C be A-algebras, with B projective separable. Then $B \otimes_A C$ is a projective separable C-algebra.*

Proof. Since B is a projective separable A-algebra, it is in particular finite projective. Then $B \otimes_A C$ is a projective A-algebra by lemma 2.1.24. Moreover, it is finitely generated as a C-module, because if $(w_1, \ldots, w_n)$ generates B over A then $(w_1 \otimes 1, \ldots, w_n \otimes 1)$ generates $B \otimes_A C$ over C.
Let now $\varphi : B \to \mathrm{Hom}_A(B, A)$ be the A-linear map defined in lemma 2.1.59 and consider the C-linear map $\varphi\otimes\mathrm{id}_C : B\otimes_A C \to \mathrm{Hom}_A(B, A)\otimes_A C$. Since B is finitely generated and projective as an A-module, by lemma 2.1.55 (condition (2)) we have an isomorphism of C-modules $\varphi_{B,A} : \mathrm{Hom}_A(B, A) \otimes_A C \to \mathrm{Hom}_C(B \otimes_A C, A \otimes_A C)$. Moreover, we have a canonical isomorphism of C-modules $\psi : A \otimes_A C \to C$, $a \otimes c \mapsto ac$, which induces an isomorphism of C-modules $\psi_* : \mathrm{Hom}_C(B \otimes_A C, A \otimes_A C) \to \mathrm{Hom}_C(B \otimes_A C, C)$, $h \mapsto \psi \circ h$. Consider now the following diagram, where φ' :

$B \otimes_A C \to \mathrm{Hom}_C(B \otimes_A C, C)$ is defined as in lemma 2.1.59, considering C instead of A and $B \otimes_A C$ instead of B.

$$\begin{array}{ccc} B \otimes_A C & \xrightarrow{\mathrm{id}_{B\otimes_A C}} & B \otimes_A C \\ \Big\downarrow{\scriptstyle \varphi \otimes \mathrm{id}_C} & & \Big\downarrow{\scriptstyle \varphi'} \\ \mathrm{Hom}_A(B, A) \otimes_A C & \xrightarrow{\psi_* \circ \varphi_{B,A}} & \mathrm{Hom}_C(B \otimes_A C, C) \end{array}$$

Let $b \in B$ and $c \in C$. We have that

$$(\psi_* \circ \varphi_{B,A})((\varphi \otimes \mathrm{id}_C)(b \otimes c)) = (\psi_* \circ \varphi_{B,A})(\varphi(b) \otimes c) = \\ = \psi_*(\varphi(b) \otimes (c\, \mathrm{id}_C)) = \psi \circ (\varphi(b) \otimes (c\, \mathrm{id}_C)) .$$

For any $x \in B$, $y \in C$, we have

$$(\psi \circ (\varphi(b) \otimes (c\, \mathrm{id}_C)))(x \otimes y) = \psi((\varphi(b)(x)) \otimes (cy)) = \psi(\mathrm{Tr}_{B/A}(bx) \otimes (cy)) = \\ = \psi(\mathrm{Tr}_{B/A}(m_{bx}) \otimes (cy)) = \mathrm{Tr}_{B/A}(m_{bx}) \cdot cy .$$

Moreover, by definition of the C-algebra structure on $B \otimes_A C$, we have $m_{(b\otimes c)(x\otimes y)} = m_{(bx)\otimes(cy)} = cym_{(bx)\otimes 1} = cy(m_{bx} \otimes \mathrm{id}_C)$. Then, using the fact that $\mathrm{Tr}_{B\otimes_A C/C}$ is C-linear (remark 2.1.48) and applying lemma 2.1.70 (with B instead of P and C instead of B), we get

$$\mathrm{Tr}_{B\otimes_A C/C}(m_{(b\otimes c)(x\otimes y)}) = \mathrm{Tr}_{B\otimes_A C/C}(cy(m_{bx\otimes \mathrm{id}_C})) = \\ = cy\, \mathrm{Tr}_{B\otimes_A C/C}(m_{bx\otimes \mathrm{id}_C}) = cy(\mathrm{Tr}_{B/A}(m_{bx}) \cdot 1) = \mathrm{Tr}_{B/A}(m_{bx}) \cdot cy .$$

Then $(\psi \circ (\varphi(b) \otimes (c\, \mathrm{id}_C)))(x \otimes y) = \mathrm{Tr}_{B\otimes_A C/C}(m_{(b\otimes c)(x\otimes y)}) = \varphi'(b \otimes c)(x \otimes y)$. So

$$(\psi_* \circ \varphi_{B,A})((\varphi \otimes \mathrm{id}_C)(b \otimes c)) = (\psi \circ (\varphi(b) \otimes (c\, \mathrm{id}_C)))(x \otimes y) = \varphi'(b \otimes c) .$$

Since this holds for any $b \in B$, $c \in C$, we have that $\psi_* \circ \varphi_{B,A} \circ (\varphi \otimes \mathrm{id}_C) = \varphi'$. Since B is a projective separable A-algebra, φ is an isomorphism. Then $\varphi \otimes \mathrm{id}_C : B \otimes_A C \to \mathrm{Hom}_A(B, A) \otimes_A C$ is an isomorphism of C-modules, with inverse $\varphi^{-1} \otimes \mathrm{id}_C$. We already knew that ψ_* and $\varphi_{B,A}$ are isomorphisms of C-modules. So φ' is an isomorphism of C-modules, because it it is the composition of isomorphisms. Hence $B \otimes_A C$ is a projective separable C-algebra. □

Proposition 2.1.72. *Let B be an A-algebra and C a faithfully flat A-algebra. Then B is a projective separable A-algebra if and only if $B \otimes_A C$ is a projective separable C-algebra.*

Proof. If B is a projective separable A-algebra, then $B \otimes_A C$ is a projective separable C-algebra by lemma 2.1.71.
Conversely, assume that $B \otimes_A C$ is a projective separable C-algebra. In particular, it is a finite projective C-algebra. Then, by proposition 2.1.57, B is a finite projective A-algebra. This implies that B is finitely presented as an A-module, by proposition 2.1.30 ((i) $\implies$ (ii)). Let $\varphi : B \to \mathrm{Hom}_A(B, A)$, $\varphi_{B,A} : \mathrm{Hom}_A(B, A) \otimes_A C \to \mathrm{Hom}_C(B \otimes_A C, A \otimes_A C)$, $\psi : A \otimes_A C \to C$ and $\varphi' : B \otimes_A C \to \mathrm{Hom}_C(B \otimes_A C, C)$ be

as in the proof of lemma 2.1.71. In the same way as in that proof, it can be shown that $\psi_* \circ \varphi_{B,A} \circ (\varphi \otimes \mathrm{id}_C) = \varphi'$. Since $B \otimes_A C$ is a projective separable C-algebra, φ' is an isomorphism of C-modules. We already knew that ψ_* is an isomorphism of C-modules. Moreover, $\varphi_{B,A}$ is also an isomorphism of C-modules, by lemma 2.1.55 (condition (1)), because B is a finitely presented A-module and C is flat. It follows that $\varphi \otimes \mathrm{id}_C = \varphi_{B,A}^{-1} \circ (\psi_*)^{-1} \circ \varphi'$ is an isomorphism of C-modules, i.e. the sequence

$$0 \otimes_A C = 0 \to B \otimes_A C \xrightarrow{\varphi \otimes \mathrm{id}_C} \mathrm{Hom}_A(B, A) \otimes_A C \to 0 = 0 \otimes_A C$$

is exact. Since C is faithfully flat, this implies that the sequence $0 \to B \xrightarrow{\varphi} \mathrm{Hom}_A(B, A) \to 0$ is also exact. This means that φ is an isomorphism. Hence B is a projective separable A-algebra. ☐

Proposition 2.1.73. *Let B be an A-algebra. If there exists a collection $(f_i)_{i \in I}$ of elements of A such that $\sum_{i \in I} f_i A = A$ and for every $i \in I$ the A_{f_i}-algebra B_{f_i} is projective separable, then B is projective separable.*

Proof. Since B_{f_i} is a projective separable A_{f_i}-algebra, it is in particular finitely generated and projective as an A_{f_i}-module, for every $i \in I$. Then, by corollary 2.1.32, B is finitely generated and projective as an A-module, i.e. it is a finite projective A-algebra. By proposition 2.1.30 ((i) $\Longrightarrow$ (ii)), we have also that B is finitely presented.

Let $i \in I$. Since B is finitely presented, by lemma 2.1.27 we have an isomorphism of A_{f_i}-modules $\varphi_{B,A}^{(i)} : \mathrm{Hom}_A(B, A)_{f_i} \to \mathrm{Hom}_{A_{f_i}}(B_{f_i}, A_{f_i})$. Let $\varphi : B \to \mathrm{Hom}_A(B, A)$ be the map defined in lemma 2.1.59 and consider its localization $\varphi_{f_i} : B_{f_i} \to \mathrm{Hom}_A(B, A)_{f_i}$, which is A_{f_i}-linear. Denote by $\varphi_i : B_{f_i} \to \mathrm{Hom}_{A_{f_i}}(B_{f_i}, A_{f_i})$ the A_{f_i}-linear map defined as in lemma 2.1.59, considering A_{f_i} instead of A and B_{f_i} instead of B. Then we have the following diagram.

$$\begin{array}{ccc} B_{f_i} & \xrightarrow{\mathrm{id}_{B_{f_i}}} & B_{f_i} \\ \Big\downarrow \varphi_{f_i} & & \Big\downarrow \varphi_i \\ \mathrm{Hom}_A(B, A)_{f_i} & \xrightarrow{\varphi_{B,A}^{(i)}} & \mathrm{Hom}_{A_{f_i}}(B_{f_i}, A_{f_i}) \end{array}$$

Recall that $B_{f_i} \cong B \otimes_A A_{f_i}$ as A_{f_i}-algebras and $\mathrm{Hom}_A(B, A)_{f_i} \cong \mathrm{Hom}_A(B, A) \otimes_A A_{f_i}$ as A_{f_i}-modules. Under these isomorphisms, the diagram we are considering corresponds to the one we considered in the proof of lemma 2.1.71. So it is commutative, as in that proof. This means that $\varphi_i = \varphi_{B,A}^{i} \circ \varphi_{f_i}$. Since B_{f_i} is a projective separable A_{f_i}-algebra, φ_i is bijective. Then, since $\varphi_{B,A}^{(i)}$ is also bijective, we have that $\varphi_{f_i} = (\varphi_{B,A}^{(i)})^{-1} \circ \varphi_i$ is bijective. Since this holds for every $i \in I$, by lemma 2.1.29(2) we get that φ is bijective, i.e. B is a projective separable A-algebra. ☐

Lemma 2.1.74. *Let B be a projective separable A-algebra and $f : B \to A$ a homomorphism of A-algebras. Then there exist an A-algebra C and an isomorphim of A-algebras $\alpha : B \to A \times C$ such that $f = p_A \circ \alpha$, where $p_A : A \times C \to A$ is the canonical projection.*

Proof. Since f is a homomorphism of A-algebras, it is in particular A-linear, i.e. $f \in \mathrm{Hom}_A(B, A)$. Let $\varphi : B \to \mathrm{Hom}_A(B, A)$ be defined as in lemma 2.1.59. Since B is projective separable, φ is bijective. So there exists a (unique) $b \in B$ such that $f = \varphi(b)$. This means that $f(x) = \mathrm{Tr}(bx)$ for any $x \in B$. In particular, $\mathrm{Tr}(b) = \mathrm{Tr}(b \cdot 1) = f(1) = 1$ (the last equality follows from the fact that f is a homomorphism of A-algebras and so in particular a ring homomorphism). Define now $C := \mathrm{Ker}(f) \subseteq B$. Then C is clearly an A-submodule of B. Notice now that f is surjective. Indeed, for any $a \in A$ we have that $f(a \cdot 1) = af(1) = a$. So the sequence of A-modules

$$0 \to C \xrightarrow{i} B \xrightarrow{f} A \to 0$$

is exact, where $i : C = \mathrm{Ker}(f) \to B$ is the canonical inclusion. Consider the A-linear map $m_b : B \to B$. For any $x \in C$, we have that $f(m_b(x)) = f(b)f(x) = 0$, because f is a ring homomorphism and $f(x) = 0$. So $m_b(x) \in \mathrm{Ker}(f) = C$. This means that $m_b(\mathrm{Im}(i)) = m_b(C) \subseteq C = \mathrm{Im}(i)$ By lemma 2.1.62, we have that $\mathrm{Tr}(b) = \mathrm{Tr}_{B/A}(m_b) = \mathrm{Tr}_{C/A}((m_b)_C) + \mathrm{Tr}_{A/A}((m_b)_A)$, where $(m_b)_C : C \to C$ is the unique A-linear map such that $i \circ (m_b)_C = m_b \circ i$ and $(m_b)_A : A \to A$ is the unique A-linear map such that $f \circ m_b = (m_b)_A \circ f$. Considering the fact that $i : C \to B$ is the canonical inclusion, we have that $(m_b)_C = (m_b)_{|C} : C \to C$. Moreover, since f is surjective, for any $y \in A$ there exists $x \in B$ such that $y = f(x)$ and so $(m_b)_A(f(x)) = f(m_b(x)) = f(bx) = f(b)f(x) = m_{f(b)}(f(x))$ (we applied the fact that f is a ring homomorphism). Then $(m_b)_A = m_{f(b)}$. Let now $x, y \in B$. We have that

$$\varphi(bx)(y) = \mathrm{Tr}(bxy) = f(xy) = f(x)f(y) = f(x)\,\mathrm{Tr}(by) = \mathrm{Tr}(f(x)by) = \varphi(f(x)b)(y)$$

(we applied the fact that the trace is A-linear, see remark 2.1.48). Then $\varphi(bx) = \varphi(f(x)b)$, which by injectivity of φ implies that $bx = f(x)b$. In particular, we have that $bx = f(x)b = 0$ for any $x \in C$, i.e. $(m_b)_{|C} = 0$. Then $\mathrm{Tr}_{C/A}((m_b)_C) = \mathrm{Tr}_{C/A}(0) = 0$ (because the trace is A-linear). So

$$\mathrm{Tr}(b) = \mathrm{Tr}_{C/A}((m_b)_C) + \mathrm{Tr}_{A/A}((m_b)_A) = \mathrm{Tr}_{A/A}(m_{f(b)}) .$$

Notice now that A is a free A-module with basis (1). By remark 2.1.50(3), we can compute the trace $\mathrm{Tr}_{A/A}$ using the definition 2.1.1. Then $\mathrm{Tr}_{A/A}(m_{f(b)}) = m_{f(b)}(1) = f(b) \cdot 1 = f(b)$. So $\mathrm{Tr}(b) = f(b)$. We have already seen that $\mathrm{Tr}(b) = 1$, so $f(b) = 1$. Consider now the map

$$\psi : A \oplus C \to B,\ (a, x) \mapsto ab + x .$$

It is immediate to check that ψ is A-linear. Let $(a, x) \in \mathrm{Ker}(\psi)$, i.e. $ab + x = \psi((a, x)) = 0$. Then $ab = -x \in C = \mathrm{Ker}(f)$. So, applying the linearity of f, we get that $0 = f(ab) = af(b) = a \cdot 1 = a$. Then $x = -ab = 0$. This proves that $\mathrm{Ker}(\psi) = 0$, i.e. ψ is injective. Let now $y \in B$. Since f is A-linear, we have that $f(y - f(y)b) = f(y) - f(y)f(b) = f(y) - f(y) \cdot 1 = 0$. So $y - f(y)b \in \mathrm{Ker}(f) = C$. Then $(f(y), y - f(y)b) \in A \oplus C$ and $\psi((f(y), y - f(y)b)) = f(y)b + y - f(y)b = y$. This proves that ψ is surjective. Then ψ is an isomorphism of A-modules. By the computation we have just performed, it is also clear that $\psi^{-1}(y) = (f(y), y - f(y)b)$

for any $y \in B$. So, if we define $\alpha := \psi^{-1} : B \to A \oplus C$, we have that $p_A \circ \alpha = f$. It remains to show that C is an A-algebra and that ψ is compatible with the multiplication (defined componentwise on $A \oplus C$). Since f is a ring homomorphism, if $x, y \in C = \mathrm{Ker}(f)$, then $f(xy) = f(x)f(y) = 0$, i.e. $xy \in \mathrm{Ker}(f) = C$. So we can restrict the multiplication from B to C. Commutativity, associativity and distributivity are inherited from the fact that B is a ring. What is a priori not clear is the fact that C has a unit element. Notice that, by what we proved above, $b^2 = f(b)b = 1 \cdot b = b$. Let now $a_1, a_2 \in A$, $x_1, x_2 \in C$. By what we proved above, $bx_1 = 0 = bx_2$. Then we have that

$$\begin{aligned}\psi((a_1, x_1))\psi((a_2, x_2)) &= (a_1 b + x_1)(a_2 b + x_2) = \\ &= a_1 a_2 b^2 + a_1 b x_2 + a_2 b x_1 + x_1 x_2 = a_1 a_2 b + x_1 x_2 = \\ &= \psi((a_1 a_2, x_1 x_2)) = \psi((a_1, x_1)(a_2, x_2)) \ .\end{aligned}$$

So ψ is compatible with the multiplication. Let now $x_0 := 1 - b = 1 - f(1)b$. By what we proved above, $x_0 \in C$ and $\psi((1, x_0)) = \psi((f(1), x_0)) = 1$. For any $x \in C$, we have that

$$\psi((1, x_0 x)) = \psi((1, x_0)(1, x)) = \psi((1, x_0))\psi((1, x)) = \psi((1, x)) \ .$$

Since ψ is injective, we must have $(1, x_0 x) = (1, x)$. Then $x_0 x = x$. This proves that x_0 is a unit element in C, which is then a ring. Consider the A-linear map $A \to C$, $a \mapsto a x_0$. This map is a ring homomorphism, because for any $a_1, a_2 \in A$ we have $(a_1 x_0)(a_2 x_0) = a_1 a_2 x_0^2 = a_1 a_2 x_0$. So C is an A-algebra, in a way that is compatible with the A-module structure inherited by B. We have that ψ is A-linear and compatible with multiplication. Moreover, we saw that $\psi((1, x_0)) = 1$. So ψ is a homomorphism of A-algebras. Then its inverse α is also a homomorphism of A-algebras. This ends the proof. □

Proposition 2.1.75. *Let B be a projective separable A-algebra. Consider $B \otimes_A B$ as a B-algebra via the second factor and consider the map $\delta : B \otimes_A B \to B$, $x \otimes y \mapsto xy$ (extended by linearity). Then there exist a B-algebra C and an isomorphism of B-algebras $\alpha : B \otimes_A B \to B \times C$ such that $\delta = p_B \circ \alpha$, where $p_B : B \times C \to B$ is the canonical projection.*

Proof. Since B is a projective separable A-algebra, $B \otimes_A B$ is a projective separable B-algebra by lemma 2.1.71. Notice that δ is well defined and A-linear, because the multiplication in B is A-bilinear. It is immediate to show that δ is actually B-linear. Moreover, by definition of the ring structure on $B \otimes_A B$, we have that δ is also a ring homomorphism. So $\delta : B \otimes_A B \to B$ is a homomorphism of B-algebras. Applying lemma 2.1.74, with $B \otimes_A B$ instead of B and B instead of A, we get the claim. □

2.2 Finite étale morphisms

We start with the definition of finite étale morphisms and of the corresponding category. Then we will study in detail the properties of these morphisms.

Definition 2.2.1. Let X, Y be two schemes and $f : Y \to X$ a morphism of schemes. We say that f is *finite étale* if there exists a cover of X by open affine subsets $(U_i = \operatorname{Spec}(A_i))_{i \in I}$ such that, for any $i \in I$, the open subscheme $f^{-1}(U_i)$ of Y is affine and equal to $\operatorname{Spec}(B_i)$, where B_i is a free separable A_i-algebra. In this situation we also say that f is a *finite étale covering* of X.
If X, Y, Z are schemes and $f : Y \to X$, $g : Z \to X$ are finite étale coverings of X, then a *morphism of coverings* from f to g is a morphism of schemes $h : Y \to Z$ such that $f = g \circ h$.

Remark 2.2.2. (1) Notice that, if $f : Y \to X$ is a morphism of schemes, $U_i = \operatorname{Spec}(A_i)$ is an open affine subscheme of X and the open subscheme $f^{-1}(U_i)$ of Y is affine, with $f^{-1}(U_i)$, then B_i is always an A_i-algebra, because the morphism of schemes $f : f^{-1}(U_i) = \operatorname{Spec}(B_i) \to U_i = \operatorname{Spec}(A_i)$ corresponds to a ring homomorphism $A_i \to B_i$.

(2) Let X be a scheme. It is immediate to check that the composition of two morphism of coverings is again a morphism of coverings. Moreover, for any finite étale covering $f : Y \to X$ we have that id_Y is clearly a morphism of coverings from f to f. This shows that finite étale coverings of X form a category. We denote this category by $\mathbf{FEt}_X$. Our goal is to prove that $\mathbf{FEt}_X$, with a suitable functor $\mathbf{FEt}_X \to \mathbf{sets}$, is a Galois category.

There are other remarkable properties that morphisms of schemes can have and we will see the connection between them and the fact of being finite étale.

Definition 2.2.3. Let X, Y be two schemes and $f : Y \to X$ a morphism of schemes. We say that f is:

(1) *affine* if there exists a cover of X by open affine subsets $(U_i)_{i \in I}$ such that $f^{-1}(U_i)$ is affine for every $i \in I$;

(2) *finite* if there is a cover of X by open affine subsets $(U_i = \operatorname{Spec}(A_i))_{i \in I}$ such that, for every $i \in I$, $f^{-1}(U_i)$ is affine and equal to $\operatorname{Spec}(B_i)$, where the A_i-algebra B_i (see remark 2.2.2(1)) is finitely generated as an A_i-module;

(3) *finite and locally free* if there exists a cover of X by open affine subsets $(U_i = \operatorname{Spec}(A_i))_{i \in I}$ such that, for every $i \in I$, $f^{-1}(U_i)$ is affine and equal to $\operatorname{Spec}(B_i)$, where the A_i-algebra B_i (see remark 2.2.2(1)) is finitely generated and free as an A_i-module;

(4) *surjective* if the corresponding map between the underlying topological spaces is surjective.

Remark 2.2.4. From the definitions, it is clear that any finite morphism of schemes is affine, any finite and locally free morphism is finite and any finite étale morphism is finite and locally free.

Lemma 2.2.5. *Let X be a scheme and consider two open affine subschemes $U = \operatorname{Spec}(A)$ and $V = \operatorname{Spec}(B)$ of X. For any $x \in U \cap V$, there exists $W \subseteq U \cap V$ such that $x \in W$ and $W = \mathrm{D}(f) = \mathrm{D}(g)$ for some $f \in A$, $g \in B$.*

Proof. Let $x \in U \cap V$. Since U and V are open, $U \cap V$ is also open. Since $U \cap V \subseteq U = \mathrm{Spec}(A)$ and distinguished open subsets form a basis of $\mathrm{Spec}(A)$, there exists $f' \in A$ such that $\mathrm{D}(f') \subseteq U \cap V$ and $x \in \mathrm{D}(f')$. We have that $\mathrm{D}(f') \subseteq V = \mathrm{Spec}(B)$ and $\mathrm{D}(f')$ is open (in U and then also in V). Since distinguished open subsets form a basis of $\mathrm{Spec}(B)$, there exists $g \in B$ such that $\mathrm{D}(g) \subseteq \mathrm{D}(f')$ and $x \in \mathrm{D}(g)$. Define $W := \mathrm{D}(g)$. Our aim is now to find an $f \in A$ such that $W = \mathrm{D}(f)$. We have that $\mathcal{O}_X(V) = \mathcal{O}_{\mathrm{Spec}(B)}(\mathrm{Spec}(B)) = B$ and $\mathcal{O}_X(\mathrm{D}(f')) = \mathcal{O}_{\mathrm{Spec}(A)}(\mathrm{D}(f')) = A_{f'}$. Since $\mathrm{D}(f') \subseteq U \cap V \subseteq V$, we can consider the restriction $\rho_{V,\mathrm{D}(f')} : \mathcal{O}_X(V) = B \to \mathcal{O}_X(\mathrm{D}(f')) = A_{f'}$. We have that $\rho_{V,\mathrm{D}(f')}(g) \in A_{f'}$. Then, by definition of localization, there exist $g' \in A$, $n \in \mathbb{N}$, such that $\rho_{V,\mathrm{D}(f')}(g) = \frac{g'}{(f')^n}$. In $V = \mathrm{Spec}(B)$, we have that $\mathrm{V}(\rho_{V,\mathrm{D}(f')}(g)) = \mathrm{V}(g) \cap \mathrm{D}(f')$ (by definition of the restriction and of vanishing sets). Recalling that $\mathrm{D}(g) \subseteq \mathrm{D}(f') \subseteq V$, we have that

$$\begin{aligned}\mathrm{D}(g) = \mathrm{D}(f') \cap \mathrm{D}(g) = \mathrm{D}(f') \cap (V \setminus \mathrm{V}(g)) = \mathrm{D}(f') \setminus (\mathrm{D}(f') \cap \mathrm{V}(g)) = \\ = \mathrm{D}(f') \setminus \mathrm{V}(\rho_{V,\mathrm{D}(f')}(g)) = \mathrm{D}(f') \setminus \mathrm{V}\left(\frac{g'}{(f')^n}\right) .\end{aligned}$$

Moreover, in $U = \mathrm{Spec}(A)$ we have that $\mathrm{V}\left(\frac{g'}{(f')^n}\right) = \mathrm{V}(g') \cap \mathrm{D}(f')$ (by definition of vanishing sets). So

$$\begin{aligned}\mathrm{D}(f') \setminus \mathrm{V}\left(\frac{g'}{(f')^n}\right) = \mathrm{D}(f') \setminus (\mathrm{V}(g') \cap \mathrm{D}(f')) = \mathrm{D}(f') \cap (U \setminus \mathrm{V}(g')) = \\ = (U \setminus \mathrm{V}(f')) \cap (U \setminus \mathrm{V}(g')) = U \setminus (\mathrm{V}(f') \cup \mathrm{V}(g')) = U \setminus \mathrm{V}(f'g') = \mathrm{D}(f'g') .\end{aligned}$$

Then, if we define $f := f'g' \in A$, we get $W = \mathrm{D}(g) = \mathrm{D}(f'g') = \mathrm{D}(f)$, as we wanted. □

Lemma 2.2.6 (Affine communication lemma, see [5], 5.3.2)**.** *Let X be a scheme and let P be a property enjoyed by some open affine subsets of X. Assume that the following two conditions are satisfied:*

(1) if an open affine subset $U = \mathrm{Spec}(A)$ has the property P, then for every $f \in A$ the open affine subset $\mathrm{Spec}(A_f) = \mathrm{D}(f) \subseteq U \subseteq X$ has P;

(2) if $U = \mathrm{Spec}(A)$ is an open affine subset of X and there exists a collection $(f_i)_{i \in I}$ of elements of A such that $\sum_{i \in I} f_i A = A$ and the open affine subset $\mathrm{Spec}(A_f) = \mathrm{D}(f) \subseteq U \subseteq X$ has the property P for every $i \in I$, then U has the property P.

If there exists a cover of X by open affine subsets $(U_i)_{i \in I}$ such that U_i enjoys the property P for every $i \in I$, then every open affine subset of X enjoys P.

Proof. Let $(U_i)_{i \in I}$ be a cover of X by open affine subsets such that $U_i = \mathrm{Spec}(A_i)$ enjoys P for every $i \in I$. Let $U = \mathrm{Spec}(A)$ be an open affine subscheme of X and consider $x \in U \subseteq X$. Since $X = \bigcup_{i \in I} U_i$, there exists $i \in I$ such that $x \in U_i$. So $x \in U \cap U_i$. By lemma 2.2.5, there exists $W_x \subseteq U \cap U_i$ such that $x \in W_x$ and $W_x = \mathrm{D}(f_x) = \mathrm{D}(g_x)$ for some $f_x \in A$, $g_x \in A_i$. Since $U_i = \mathrm{Spec}(A_i)$ enjoys

P, $\mathrm{Spec}(A_{g_x}) = \mathrm{D}(g_x)$ enjoys P, by the first assumption. Consider now $(f_x)_{x\in U}$, which is a collection of elements of A. Since $x \in \mathrm{D}(f_x)$ for any $x \in U$, we have that $U = \bigcup_{x\in U} \mathrm{D}(f_x)$. Consider now the ideal $\sum_{x\in U} f_x A \subseteq A$. If it was a proper ideal, there would exist a maximal ideal $\mathfrak{m}$ such that $\sum_{x\in U} f_x A \subseteq \mathfrak{m}$, i.e. $f_x \in \mathfrak{m}$ for any $x \in U$. Then $\mathfrak{m} \in \mathrm{Spec}(A) = U$, but $\mathfrak{m} \notin \mathrm{D}(f_x)$, for any $x \in U$. This is a contradiction. So $\sum_{x\in U} f_x A = A$. Since $\mathrm{D}(f_x) = \mathrm{D}(g_x)$ enjoys P for every $x \in U$, it follows that U enjoys P, by the second assumption. □

Lemma 2.2.7. *Let $(X, \mathcal{O}_X)$ be a scheme and let $f \in \mathcal{O}_X(X)$. We define*

$$X_f := \{x \in X \mid f_x \notin \mathfrak{m}_{X,x}\} = \{x \in X \mid f_x \in \mathcal{O}_{X,x} \backslash \mathfrak{m}_{X,x} = \mathcal{O}_{X,x}^\times\} \subseteq X \ .$$

Then we have that:

(1) X_f is open;

(2) $\rho_{X,X_f}(f) \in \mathcal{O}_X(X_f)^\times$, where $\rho_{X,X_f} : \mathcal{O}_X(X) \to \mathcal{O}_X(X_f)$ is the restriction map;

(3) if there exists a finite cover $(U_i = \mathrm{Spec}(A_i))_{i=1,\dots,n}$ of X by open affine subsets such that for every $i, j = 1, \dots, n$ the intersection $U_i \cap U_j$ is a finite union of open affine subsets, then the induced ring homomorphism $\widetilde{\rho} : \mathcal{O}_X(X)_f \to \mathcal{O}_X(X_f)$ is an isomorphism.

Proof. (1) Let $x \in X_f$. By definition, this means that $f_x \in \mathcal{O}_{X,x}^\times$. Then there exists $\varphi \in \mathcal{O}_{X,x}$ such that $f_x\varphi = 1$. By definition of stalk, there exist an open neighbourhood U of x in X and $g \in \mathcal{O}_X(U)$ such that $\varphi = g_x$. Then $f_x g_x = 1 = 1_x$. Again by definition of stalk, this implies that there exists an open neighbourhood $V \subseteq X \cap U = U$ of x such that $\rho_{X,V}(f)\rho_{U,V}(g) = 1$ (we denote by $\rho_{X,V}$ and $\rho_{U,V}$ the restriction maps). Then, for any $x' \in V$ we have that $f_{x'}g_{x'} = \rho_{X,V}(f)_{x'}\rho_{U,V}(g)_{x'} = 1_{x'} = 1$ and so $f_{x'} \in \mathcal{O}_{X,x'}^\times$, i.e. $x' \in X_f$. So $V \subseteq X_f$. This proves that X_f is open.

(2) From the proof of point (1), for every $x \in X_f$ there exist an open neighbourhood $V_x \subseteq X_f$ of x and $g^{(x)} \in \mathcal{O}_X(V_x)$ such that $\rho_{X,V_x}(f) \cdot g^{(x)} = 1$. Then we have that $X_f = \bigcup_{x\in X_f} V_x$. Consider the collection $\left(g^{(x)}\right)_{x\in X_f} \subseteq \prod_{x\in X_f} \mathcal{O}_X(V_x)$. Let $x, x' \in X_f$ and consider $\rho_{V_x,V_x\cap V_{x'}}\left(g^{(x)}\right), \rho_{V_{x'},V_x\cap V_{x'}}\left(g^{(x')}\right) \in \mathcal{O}_X(V_x \cap V_{x'})$. Let $x'' \in V_x \cap V_{x'}$. Since $x'' \in V_x$ and $\rho_{X,V_x}(f) \cdot g^{(x)} = 1$, we have that $f_{x''}\left(g^{(x)}\right)_{x''} = \rho_{X,V_x}(f)_{x''}\left(g^{(x)}\right)_{x''} = 1_{x''} = 1$. Analogously, we have $f_{x''}\left(g^{(x')}\right)_{x''} = \rho_{X,V_{x'}}(f)_{x''}\left(g^{(x')}\right)_{x''} = 1_{x''} = 1$. By uniqueness of the inverse, this implies that $\left(g^{(x)}\right)_{x''} = \left(g^{(x')}\right)_{x''}$ By definition of stalk, there exists an open neighbourhood $W_{x''}$ of x'' in $V_x \cap V_{x'}$ such that $\rho_{V_x,W_{x''}}\left(g^{(x)}\right) = \rho_{V_{x'},W_{x''}}\left(g^{(x')}\right)$. We have that $V_x \cap V_{x'} = \bigcup_{x''\in V_x\cap V_{x'}} W_{x''}$. Then, by definition

of sheaf, we get $\rho_{V_x,V_x\cap V_{x'}}\left(g^{(x)}\right)=\rho_{V_{x'},V_x\cap V_{x'}}\left(g^{(x')}\right)$, because

$$\rho_{V_x\cap V_{x'},W_{x''}}\left(\rho_{V_x,V_x\cap V_{x'}}\left(g^{(x)}\right)\right)=\rho_{V_x,W_{x''}}\left(g^{(x)}\right)= \\ =\rho_{V_{x'},W_{x''}}\left(g^{(x')}\right)=\rho_{V_x\cap V_{x'},W_{x''}}\left(\rho_{V_{x'},V_x\cap V_{x'}}\left(g^{(x')}\right)\right)$$

for every $x''\in V_x\cap V_{x'}$. By definition of sheaf, there exists $g\in\mathcal{O}_X(X_f)$ such that $g^{(x)}=\rho_{X_f,V_x}(g)$ for every $x\in X$. Then $\rho_{X,V_x}(fg)=\rho_{X,V_x}(f)\rho_{X,V_x}(g)=\rho_{X,V_x}(f)\cdot g^{(x)}=1=\rho_{X,V_x}(1)$ for every $x\in X_f$ (because the restriction maps are ring homomorphisms). By definition of sheaf, this implies that $fg=1$ (because $X_f=\bigcup_{x\in X_f}V_x$). Then $f\in\mathcal{O}_X(X_f)^\times$.

(3) By point (2), $\rho_{X,X_f}(f^n)=\rho_{X,X_f}(f)^n\in\mathcal{O}_X(X_f)^\times$ for every $n\geq 0$, i.e. $\rho_{X,X_f}(S_f)\subseteq\mathcal{O}_X(X_f)^\times$. By the universal property of the localization, the ring homomorphism $\rho_{X,X_f}:\mathcal{O}_X(X)\to\mathcal{O}_X(X_f)$ induces indeed a ring homomorphism $\widetilde{\rho}:\mathcal{O}_X(X)_f\to\mathcal{O}_X(X_f)$.
Consider $i\in\{1,\dots,n\}$ and define

$$f_i:=\rho_{X,U_i}(f)\in\mathcal{O}_X(U_i)=\mathcal{O}_{\mathrm{Spec}(A_i)}(\mathrm{Spec}(A_i))=A_i\ .$$

We have that

$$X_f\cap U_i=\{x\in U_i\mid f_x\notin\mathfrak{m}_{X,x}\}=\{x\in U_i\mid (f_i)_x=\rho_{X,U_i}(f)_x\notin\mathfrak{m}_{X,x}\}= \\ =\{\mathfrak{p}\in\mathrm{Spec}(A_i)\mid (f_i)_{\mathfrak{p}}\notin\mathfrak{m}_{\mathrm{Spec}(A_i),\mathfrak{p}}\}=(\mathrm{Spec}(A_i))_{f_i}\ .$$

Identifying $\mathcal{O}_{\mathrm{Spec}(A_i),\mathfrak{p}}$ with $(A_i)_{\mathfrak{p}}$ and $\mathfrak{m}_{\mathrm{Spec}(A_i),\mathfrak{p}}$ with $\mathfrak{p}_{\mathfrak{p}}$ for every $\mathfrak{p}\in\mathrm{Spec}(A_i)$, we get that

$$(\mathrm{Spec}(A_i))_{f_i}=\left\{\mathfrak{p}\in\mathrm{Spec}(A_i)\ \middle|\ \frac{f_i}{1}\notin\mathfrak{p}_{\mathfrak{p}}\right\}=\{\mathfrak{p}\in\mathrm{Spec}(A_i)\mid f_i\notin\mathfrak{p}\}=\mathrm{D}(f_i)\ .$$

So $X_f\cap U_i=\mathrm{D}(f_i)$. The restriction map

$$\rho_{U_i,\mathrm{D}(f_i)}:\mathcal{O}_X(U_i)=A_i\to\mathcal{O}_X(\mathrm{D}(f_i))=\mathcal{O}_{\mathrm{Spec}(A_i)}(\mathrm{D}(f_i))$$

induces a ring homomorphism $\widetilde{\rho}_i:(A_i)_{f_i}\to\mathcal{O}_{\mathrm{Spec}(A_i)}(\mathrm{D}(f_i))$ and we know that this is an isomorphism by the properties of affine schemes. This holds for every $i=1,\dots,n$. Let now $\frac{g}{f^m}\in\mathrm{Ker}(\widetilde{\rho})\subseteq\mathcal{O}_X(X)_f$, with $g\in\mathcal{O}_X(X)$ and $m\in\mathbb{N}$. Then $\rho_{X,X_f}(g)\rho_{X,X_f}(f)^{-m}=\widetilde{\rho}\left(\frac{g}{f^m}\right)=0$. Multiplying by $\rho_{X,X_f}(f)^m$, we get that $\rho_{X,X_f}(g)=0$. Let $i\in\{1,\dots,n\}$. Then

$$\rho_{U_i,\mathrm{D}(f_i)}(\rho_{X,U_i}(g))=\rho_{X,\mathrm{D}(f_i)}(g)=\rho_{X_f,\mathrm{D}(f_i)}(\rho_{X,X_f}(g))=\rho_{X_f,\mathrm{D}(f_i)}(0)=0\ .$$

This implies that $\widetilde{\rho}_i\left(\frac{\rho_{X,U_i}(g)}{1}\right)=\rho_{U_i,\mathrm{D}(f_i)}(g)=0$. Since $\widetilde{\rho}_i$ is an isomorphism, we have that $\frac{\rho_{X,U_i}(g)}{1}=0$ in $(A_i)_{f_i}$. This means that there exists $r_i\in\mathbb{N}$ such that $f_i^{r_i}\rho_{X,U_i}(g) = 0$. Define $r := \max_{i=1,\dots,n} r_i$. Then, since ρ_{X,U_i} is a ring homomorphism,

$$\rho_{X,U_i}(f^r g) = \rho_{X,U_i}(f)^r \rho_{X,U_i}(g) = f_i^r \rho_{X,U_i}(g) = \\ = f_i^{r-r_i} f_i^{r_i} \rho_{X,U_i}(g) = f_i^{r-r_i} \cdot 0 = 0$$

for every $i = 1, \dots, n$. Since $X = \bigcup_{i=1}^n U_i$, this implies that $f^r g = 0$, by definition of sheaf. Then $\frac{g}{f^m} = \frac{f^r g}{f^{m+r}} = 0$. So $\mathrm{Ker}(\widetilde{\rho}) = 0$, i.e. $\widetilde{\rho}$ is injective. Notice that we used only the fact that we had a finite cover: for injectivity the assumption about the intersections is not needed.
On the other hand, let $g \in \mathcal{O}_X(X_f)$. Consider $i \in \{1, \dots, n\}$ and $\rho_{X_f,\mathrm{D}(f_i)}(g) \in \mathcal{O}_X(\mathrm{D}(f_i)) = \mathcal{O}_{\mathrm{Spec}(A_i)}(\mathrm{D}(f_i))$. Since $\widetilde{\rho}_i$ is an isomorphism, there exist $h_i \in A_i$, $m_i \in \mathbb{N}$ such that $\rho_{X_f,\mathrm{D}(f_i)}(g) = \widetilde{\rho}_i\left(\frac{h_i}{f_i^{m_i}}\right)$. Define $m := \max_{i=1,\dots,n} m_i$. Then, for every $i = 1, \dots, n$, we have that $\frac{h_i}{f_i^{m_i}} = \frac{f_i^{m-m_i} h_i}{f_i^m} = \frac{\widetilde{h}_i}{f_i^m}$, where we defined $\widetilde{h}_i := f_i^{m-m_i} h_i \in A_i$. So

$$\rho_{X_f,\mathrm{D}(f_i)}(g) = \widetilde{\rho}_i\left(\frac{h_i}{f_i^{m_i}}\right) = \widetilde{\rho}_i\left(\frac{\widetilde{h}_i}{f_i^m}\right) = \rho_{U_i,\mathrm{D}(f_i)}\left(\widetilde{h}_i\right) \rho_{U_i,\mathrm{D}(f_i)}(f_i)^{-m} .$$

Let now $i, j \in \{1, \dots, n\}$. By assumption, we can write $U_i \cap U_j = \bigcup_{k=1}^{K_{ij}} V_{ijk}$, with $K_{ij} \in \mathbb{N}$ and V_{ijk} affine for every $k = 1, \dots, K_{ij}$. Let $k \in \{1, \dots, K_{ij}\}$ and $V_{ijk} = \mathrm{Spec}(B_{ijk})$. We have that $V_{ijk} \cap X_f \subseteq U_i \cap X_f = \mathrm{D}(f_i)$ and $V_{ijk} \cap X_f \subseteq U_j \cap X_f = \mathrm{D}(f_j)$. Then

$$\rho_{X_f,V_{ijk}\cap X_f}(g) = \rho_{\mathrm{D}(f_i),V_{ijk}\cap X_f}(\rho_{X_f,\mathrm{D}(f_i)}(g)) = \\ = \rho_{\mathrm{D}(f_i),V_{ijk}\cap X_f}\left(\rho_{U_i,\mathrm{D}(f_i)}\left(\widetilde{h}_i\right) \rho_{U_i,\mathrm{D}(f_i)}(f_i)^{-m}\right) = \\ = \rho_{\mathrm{D}(f_i),V_{ijk}\cap X_f}\left(\rho_{U_i,\mathrm{D}(f_i)}\left(\widetilde{h}_i\right)\right) \cdot \rho_{\mathrm{D}(f_i),V_{ijk}\cap X_f}(\rho_{U_i,\mathrm{D}(f_i)}(\rho_{X,U_i}(f)))^{-m} = \\ = \rho_{U_i,V_{ijk}\cap X_f}\left(\widetilde{h}_i\right) \rho_{X,V_{ijk}\cap X_f}(f)^{-m}$$

and

$$\rho_{X_f,V_{ijk}\cap X_f}(g) = \rho_{\mathrm{D}(f_j),V_{ijk}\cap X_f}(\rho_{X_f,\mathrm{D}(f_j)}(g)) = \\ = \rho_{\mathrm{D}(f_j),V_{ijk}\cap X_f}\left(\rho_{U_j,\mathrm{D}(f_j)}\left(\widetilde{h}_j\right) \rho_{U_j,\mathrm{D}(f_j)}(f_j)^{-m}\right) = \\ = \rho_{\mathrm{D}(f_j),V_{ijk}\cap X_f}\left(\rho_{U_j,\mathrm{D}(f_j)}\left(\widetilde{h}_j\right)\right) \cdot \rho_{\mathrm{D}(f_j),V_{ijk}\cap X_f}(\rho_{U_j,\mathrm{D}(f_j)}(\rho_{X,U_j}(f)))^{-m} = \\ = \rho_{U_j,V_{ijk}\cap X_f}\left(\widetilde{h}_j\right) \rho_{X,V_{ijk}\cap X_f}(f)^{-m} .$$

So $\rho_{U_i,V_{ijk}\cap X_f}\left(\widetilde{h}_i\right) \rho_{X,V_{ijk}\cap X_f}(f)^{-m} = \rho_{U_j,V_{ijk}\cap X_f}\left(\widetilde{h}_j\right) \rho_{X,V_{ijk}\cap X_f}(f)^{-m}$ and, multiplying by $\rho_{X,V_{ijk}\cap X_f}(f)^m$, we get that

$$\rho_{U_i\cap U_j\cap X_f,V_{ijk}\cap X_f}\left(\rho_{U_i,U_i\cap U_j\cap X_f}\left(\widetilde{h}_i\right)\right) = \rho_{U_i,V_{ijk}\cap X_f}\left(\widetilde{h}_i\right) = \\ = \rho_{U_j,V_{ijk}\cap X_f}\left(\widetilde{h}_j\right) = \rho_{U_i\cap U_j\cap X_f,V_{ijk}\cap X_f}\left(\rho_{U_j,U_i\cap U_j\cap X_f}\left(\widetilde{h}_j\right)\right) .$$

Since this holds for any $k = 1, \dots, K_{ij}$ and $U_i \cap U_j \cap X_f = \left(\bigcup_{k=1}^{K_{ij}} V_{ijk} \right) \cap X_f = \bigcup_{k=1}^{K_{ij}} (V_{ijk} \cap X_f)$, by definition of sheaf $\rho_{U_i, U_i \cap U_j \cap X_f} \left(\widetilde{h}_i \right) = \rho_{U_j, U_i \cap U_j \cap X_f} \left(\widetilde{h}_j \right)$. Notice now that

$$\begin{aligned} U_i \cap U_j \cap X_f = \{x \in U_i \cap U_j \mid f_x \notin \mathfrak{m}_{X,x}\} = \\ = \{x \in U_i \cap U_j \mid \rho_{X, U_i \cap U_j}(f)_x \notin \mathfrak{m}_{U_i \cap U_j, x}\} = (U_i \cap U_j)_{f_{ij}} \ , \end{aligned}$$

where we defined $f_{ij} := \rho_{X, U_i \cap U_j}(f)$. Then the restriction map

$$\begin{aligned} \rho_{U_i \cap U_j, U_i \cap U_j \cap X_f} : \mathcal{O}_X(U_i \cap U_j) = \mathcal{O}_{U_i \cap U_j}(U_i \cap U_j) \to \\ \to \mathcal{O}_X(U_i \cap U_j \cap X_f) = \mathcal{O}_{U_i \cap U_j}\left((U_i \cap U_j)_{f_{ij}}\right) \end{aligned}$$

induces a ring homomorphism

$$\widetilde{\rho}_{ij} : \mathcal{O}_{U_i \cap U_j}(U_i \cap U_j)_{f_{ij}} \to \mathcal{O}_{U_i \cap U_j}\left((U_i \cap U_j)_{f_{ij}}\right) \ ,$$

which is injective by what we proved above, because $U_i \cap U_j$ admits a finite cover by open affine subsets and this is the only assumption that we used to prove that $\widetilde{\rho}$ is injective. Now we have that

$$\begin{aligned} \widetilde{\rho}_{ij} \left(\frac{\rho_{U_i, U_i \cap U_j}\left(\widetilde{h}_i\right)}{1} \right) = \rho_{U_i \cap U_j, U_i \cap U_j \cap X_f}\left(\rho_{U_i, U_i \cap U_j}\left(\widetilde{h}_i\right)\right) = \\ = \rho_{U_i, U_i \cap U_j \cap X_f}\left(\widetilde{h}_i\right) = \rho_{U_j, U_i \cap U_j \cap X_f}\left(\widetilde{h}_j\right) = \\ = \rho_{U_i \cap U_j, U_i \cap U_j \cap X_f}\left(\rho_{U_j, U_i \cap U_j}\left(\widetilde{h}_j\right)\right) = \widetilde{\rho}_{ij}\left(\frac{\rho_{U_j, U_i \cap U_j}\left(\widetilde{h}_j\right)}{1} \right) \ . \end{aligned}$$

Since $\widetilde{\rho}_{ij}$ is injective, this implies that $\frac{\rho_{U_i, U_i \cap U_j}(\widetilde{h}_i)}{1} = \frac{\rho_{U_j, U_i \cap U_j}(\widetilde{h}_j)}{1}$ in $\mathcal{O}_X(U_i \cap U_j)_{\rho_{X, U_i \cap U_j}(f)}$. This means that there exists $r_{ij} \in \mathbb{N}$ such that

$$f_{ij}^{r_{ij}} \left(\rho_{U_i, U_i \cap U_j}\left(\widetilde{h}_i\right) \cdot 1 - \rho_{U_j, U_i \cap U_j}\left(\widetilde{h}_j\right) \cdot 1 \right) = 0 \ ,$$

i.e. $f_{ij}^{r_{ij}} \rho_{U_i, U_i \cap U_j}\left(\widetilde{h}_i\right) = f_{ij}^{r_{ij}} \rho_{U_j, U_i \cap U_j}\left(\widetilde{h}_j\right)$. Let $r := \max_{i,j=1,\dots,n} r_{ij}$. Then

$$\begin{aligned} \rho_{U_i, U_i \cap U_j}\left(f_i^r \widetilde{h}_i\right) = \rho_{U_i, U_i \cap U_j}(f_i)^r \rho_{U_i, U_i \cap U_j}\left(\widetilde{h}_i\right) = \\ = \rho_{U_i, U_i \cap U_j}(\rho_{U, U_i}(f))^r \rho_{U_i, U_i \cap U_j}\left(\widetilde{h}_i\right) = f_{ij}^r \rho_{U_i, U_i \cap U_j}\left(\widetilde{h}_i\right) = \\ = f_{ij}^{r - r_{ij}} f_{ij}^{r_{ij}} \rho_{U_i, U_i \cap U_j}\left(\widetilde{h}_i\right) = f_{ij}^{r - r_{ij}} f_{ij}^{r_{ij}} \rho_{U_j, U_i \cap U_j}\left(\widetilde{h}_j\right) = \\ = f_{ij}^r \rho_{U_j, U_i \cap U_j}\left(\widetilde{h}_j\right) = \rho_{U_j, U_i \cap U_j}(\rho_{U, U_j}(f))^r \rho_{U_j, U_i \cap U_j}\left(\widetilde{h}_j\right) = \\ = \rho_{U_j, U_i \cap U_j}(f_j)^r \rho_{U_j, U_i \cap U_j}\left(\widetilde{h}_j\right) = \rho_{U_j, U_i \cap U_j}\left(f_j^r \widetilde{h}_j\right) \end{aligned}$$

for every $i, j = 1, \dots, n$. Then, considering $\left(f_i^r \widetilde{h}_i\right) \subseteq \prod_{i=1}^n \mathcal{O}_X(U_i)$, we get (by definition of sheaf) that there exists $h \in \mathcal{O}_X(X)$ such that $\rho_{X,U_i}(h) = f_i^r \widetilde{h}_i$ for every $i = 1, \dots, n$. Then

$$\begin{gathered}
\rho_{X_f,\mathrm{D}(f_i)}\left(\widetilde{\rho}\left(\frac{h}{f^{m+r}}\right)\right) = \rho_{X_f,\mathrm{D}(f_i)}(\rho_{X,X_f}(h)\rho_{X,X_f}(f)^{-m-r}) = \\
= \rho_{X_f,\mathrm{D}(f_i)}(\rho_{X,X_f}(h))\rho_{X_f,\mathrm{D}(f_i)}(\rho_{X,X_f}(f))^{-m-r} = \\
= \rho_{X,\mathrm{D}(f_i)}(h)\rho_{X,\mathrm{D}(f_i)}(f)^{-m-r} = \rho_{U_i,\mathrm{D}(f_i)}(\rho_{X,U_i}(h))\rho_{U_i,\mathrm{D}(f_i)}(\rho_{X,U_i}(f))^{-m-r} = \\
= \rho_{U_i,\mathrm{D}(f_i)}\left(f_i^r \widetilde{h}_i\right)\rho_{U_i,\mathrm{D}(f_i)}(f_i)^{-m-r} = \\
= \rho_{U_i,\mathrm{D}(f_i)}(f_i)^r \rho_{U_i,\mathrm{D}(f_i)}\left(\widetilde{h}_i\right)\rho_{U_i,\mathrm{D}(f_i)}(f_i)^{-m-r} = \\
= \rho_{U_i,\mathrm{D}(f_i)}\left(\widetilde{h}_i\right)\rho_{U_i,\mathrm{D}(f_i)}(f_i)^{-m} = \rho_{X_f,\mathrm{D}(f_i)}(g)
\end{gathered}$$

for any $i = 1, \dots, n$. Since $X_f = \bigcup_{i=1}^n (X_f \cap U_i) = \bigcup_{i=1}^n \mathrm{D}(f_i)$, by definition of sheaf we get that $\widetilde{\rho}\left(\frac{h}{f^{m+r}}\right) = g$. Hence $\widetilde{\rho}$ is surjective.

□

Remark 2.2.8. If $(X, \mathcal{O}_X) = \mathrm{Spec}(A)$ is an affine scheme, then for any $f \in \mathcal{O}_X(X) = A$ we have that $X_f = \mathrm{D}(f)$ (see the proof of 2.2.7(3)). Then the lemma 2.2.7 is a generalization of the fact that $\mathcal{O}_{\mathrm{Spec}(A)}(\mathrm{D}(f)) \cong A_f$.

Lemma 2.2.9. *Let X be a scheme and denote by $A := \mathcal{O}_X(X)$ the ring of global sections. Then X is affine (and isomorphic to* $\mathrm{Spec}(A)$*) if and only if there exists a collection $(f_i)_{i\in I}$ of elements of A such that $\sum_{i\in I} f_i A = A$ and X_{f_i} (defined as in lemma 2.2.7) is affine for every $i \in I$.*

Proof. If X is affine, consider $I = \{1\}$ and $f_1 = 1 \in A$. Then we have that $\sum_{i\in I} f_i A = f_1 A = 1A = A$ and

$$X_{f_1} = X_1 = \{x \in X \mid 1 = 1_x \notin \mathfrak{m}_{X,x}\} = X$$

is affine (the last equality follows from the fact that $\mathfrak{m}_{X,x}$ is a proper ideal of $\mathcal{O}_{X,x}$). Moreover, if $X \cong \mathrm{Spec}(A')$, we have that $A' = \mathcal{O}_{\mathrm{Spec}(A')}(\mathrm{Spec}(A')) \cong \mathcal{O}_X(X) = A$. So $X \cong \mathrm{Spec}(A') \cong \mathrm{Spec}(A)$.

Conversely, let $(f_i)_{i\in I}$ be a collection of elements of A such that $\sum_{i\in I} f_i A = A$ and X_{f_i} is affine for every $i \in I$. For any open affine subset $U = \mathrm{Spec}(B) \subseteq X$, the restriction map $\rho_{X,U} : \mathcal{O}_X(X) = A \to \mathcal{O}_X(U) = \mathcal{O}_{\mathrm{Spec}(B)}(\mathrm{Spec}(B)) = B$ (which is a ring homomorphism) induces a morphism of schemes $\varphi_U : \mathrm{Spec}(B) = U \to \mathrm{Spec}(A)$. These morphisms are all compatible with each other. Indeed, if $U_1 = \mathrm{Spec}(B_1)$ and $U_2 = \mathrm{Spec}(B_2)$ are two open affine subsets of X, then we can cover the intersection $U_1 \cap U_2$ with open affine subsets (distinguished open subsets of $\mathrm{Spec}(B_1)$ or of $\mathrm{Spec}(B_2)$) and we have that $(\varphi_{U_1})_{|V} = \varphi_V = (\varphi_{U_2})_{|V}$ for every open affine subset $V \subseteq U_1 \cap U_2$. So $(\varphi_{U_1})_{|U_1\cap U_2} = (\varphi_{U_2})_{|U_1\cap U_2}$. Then, since X is covered by its open affine subsets, we can glue the morphisms φ_U's and get a morphism of schemes $\varphi : X \to \mathrm{Spec}(A)$. Our aim is now to prove that φ is an isomorphism.

Let $\varphi^{\#} : \mathcal{O}_{\mathrm{Spec}(A)}(\mathrm{Spec}(A)) = A \to \mathcal{O}_X(X) = A$ be the ring homomorphism induced by φ. Let $a \in A = \mathcal{O}_X(X)$ and consider $\varphi^{\#}(a) \in \mathcal{O}_X(X)$. For every open affine subset U of X, we have that $\rho_{X,U} \circ \varphi^{\#} = \rho_{X,U}$ by definition of φ, so $\rho_{X,U}(\varphi^{\#}(a)) = \rho_{X,U}(a)$. Since X is covered by its open affine subsets, by definition of sheaf we must have $\varphi^{\#}(a) = a$. Since this holds for every $a \in A$, it follows that $\varphi^{\#} = \mathrm{id}_A$. Fix now $j \in I$. Recalling that $\mathrm{D}(f_j) = \mathrm{Spec}(A)_{f_j}$ (see remark 2.2.8 or the proof of lemma 2.2.7(3)), we have that

$$\begin{aligned}\varphi^{-1}(\mathrm{D}(f_j)) = \{x \in X \mid \varphi(x) \in \mathrm{D}(f_j) = \mathrm{Spec}(A)_{f_j}\} = \\ = \{x \in X \mid (f_j)_{\varphi(x)} \notin \mathfrak{m}_{\mathrm{Spec}(A),\varphi(x)}\} = \\ = \{x \in X \mid (f_j)_x = (\varphi^{\#}(f_j))_x \notin \mathfrak{m}_{X,x}\} = X_{f_j} \ ,\end{aligned}$$

by definition of morphism of schemes. By assumption, X_{f_j} is affine. Then, by definition of φ, we have that $\varphi_{|_{\varphi^{-1}(\mathrm{D}(f_j))}} = \varphi_{X_{f_j}} : X_{f_j} \to \mathrm{Spec}(A)$ corresponds to the restriction $\rho_{X,X_{f_j}} : \mathcal{O}_X(X) = A \to \mathcal{O}_X(X_{f_j})$. So $\varphi_{X_{f_j}} : X_{f_j} = \varphi^{-1}(\mathrm{D}(f_j)) \to \mathrm{D}(f_j)$ corresponds to the induced ring homomorphism

$$\widetilde{\rho}_j : \mathcal{O}_X(X)_{f_j} \to \mathcal{O}_X(X_{f_j}) \ .$$

We prove now that X satisfies the assumptions of lemma 2.2.7(3). Since $\sum_{i\in I} f_i A = A$, there exist $n \in \mathbb{N}$, $i_1, \dots, i_k \in I$ and $\lambda_1, \dots, \lambda_n \in A$ such that $1 = \sum_{k=1}^{n} \lambda_k f_{i_k}$. Let now $x \in X$. Assume by contradiction that $x \notin X_{f_{i_k}}$ for any $k \in \{1, \dots, n\}$. This means that $(f_{i_k})_x \in \mathfrak{m}_{X,x}$ for any $k \in \{1, \dots, n\}$. Then $1_x = \sum_{k=1}^{n} (\lambda_k)_x (f_{i_k})_x \in \mathfrak{m}_{X,x}$. This is a contradiction, because $\mathfrak{m}_{X,x}$ is a proper ideal of $\mathcal{O}_{X,x}$. Then there exists $k \in \{1, \dots, n\}$ such that $x \in X_{f_{i_k}}$. This shows that $X = \bigcup_{k=1}^{n} X_{f_{i_k}}$. By assumption, $X_{f_{i_k}}$ is affine for every $k = 1, \dots, n$. Let $h, k \in \{1, \dots, n\}$ and consider the intersection $X_{f_{i_h}} \cap X_{f_{i_k}}$. If $X_{f_{i_h}} = \mathrm{Spec}(B_h)$, as in the proof of lemma 2.2.7(3) we have that

$$X_{f_{i_h}} \cap X_{f_{i_k}} = \mathrm{Spec}(B_h) \cap X_{f_{i_k}} = \mathrm{D}(\rho_{X,X_{f_{i_h}}}(f_{i_k})) = \mathrm{Spec}\left((B_h)_{\rho_{X,X_{f_{i_h}}}(f_{i_k})}\right)$$

is affine. Then by lemma 2.2.7(3) we have that $\widetilde{\rho}_j$ is an isomorphism and so the corresponding morphism of schemes $\varphi_{X_{f_j}} : X_{f_j} = \varphi^{-1}(\mathrm{D}(f_j)) \to \mathrm{D}(f_j)$ is an isomorphism. So we can consider its inverse $\psi_j := \varphi^{-1}_{X_{f_j}} : \mathrm{D}(f_j) \to X_{f_j}$. The morphisms ψ_j's are all compatible with each other. Indeed, for any $i, j \in I$ we have that

$$\begin{aligned}(\psi_i)_{|_{\mathrm{D}(f_i)\cap \mathrm{D}(f_j)}} = \left(\varphi^{-1}_{X_{f_i}}\right)_{|_{\mathrm{D}(f_i)\cap \mathrm{D}(f_j)}} = \left((\varphi_{X_{f_i}})_{|_{X_{f_i}\cap X_{f_j}}}\right)^{-1} = \left(\varphi_{|_{X_{f_i}\cap X_{f_j}}}\right)^{-1} = \\ = \left((\varphi_{X_{f_j}})_{|_{X_{f_i}\cap X_{f_j}}}\right)^{-1} = \left(\varphi^{-1}_{X_{f_j}}\right)_{|_{\mathrm{D}(f_i)\cap \mathrm{D}(f_j)}} = (\psi_j)_{|_{\mathrm{D}(f_i)\cap \mathrm{D}(f_j)}} \ .\end{aligned}$$

Let $\mathfrak{p} \in \mathrm{Spec}(A)$. In particular, $\mathfrak{p}$ is a proper ideal of A. Then there exists $i \in I$ such that $f_i \notin \mathfrak{p}$, because otherwise we would have $A = \sum_{i\in I} f_i A \subseteq \mathfrak{p}$. This means that $\mathfrak{p} \in \mathrm{D}(f_i)$. Then $\mathrm{Spec}(A) = \bigcup_{i\in I} \mathrm{D}(f_i)$. So we can glue the ψ_j's and get a morphism of schemes $\psi : \mathrm{Spec}(A) \to X$. We have that φ and ψ are inverse to each other, because this is true considering the restrictions to $\varphi^{-1}(\mathrm{D}(f_i))$ and $\mathrm{D}(f_i)$ for every $i \in I$. So φ is an isomorphism of schemes and $X \cong \mathrm{Spec}(A)$ is affine. □

Lemma 2.2.10. *Let X, Y be two schemes and $f : Y \to X$ a morphism of schemes. We have that:*

(1) f is affine if and only if $f^{-1}(U)$ is affine for every open affine subscheme U of X;

(2) f is finite if and only if for every open affine subscheme $U = \mathrm{Spec}(A)$ of X the open subscheme $f^{-1}(U)$ of Y is affine and equal to $\mathrm{Spec}(B)$, where the A-algebra B is finitely generated as an A-module;

(3) f is finite and locally free if and only if for every open affine subscheme $U = \mathrm{Spec}(A)$ of X the open subscheme $f^{-1}(U)$ of Y is affine and equal to $\mathrm{Spec}(B)$, where B is a finite projective A-algebra;

(4) f is finite étale if and only if for every open affine subscheme $U = \mathrm{Spec}(A)$ of X the open subscheme $f^{-1}(U)$ of Y is affine and equal to $\mathrm{Spec}(B)$, where B is a projective separable A-algebra.

Proof. (1) If $f^{-1}(U)$ is affine for every open affine subscheme U of X, then every cover of X by open affine subsets satisfies the condition required in the definition and such a cover exists by definition of scheme. So f is affine.
Conversely, assume that f is affine. Then there exists a cover of X by open affine subsets $(U_i)_{i\in I}$ such that $f^{-1}(U_i)$ is affine. We want to prove that the property of having affine preimage satisfies the assumptions of the affine communication lemma. Let $U = \mathrm{Spec}(A)$ be an open affine subscheme of X such that $f^{-1}(U)$ is affine and $f^{-1}(U) = \mathrm{Spec}(B)$. The morphism $f : f^{-1}(U) = \mathrm{Spec}(B) \to U = \mathrm{Spec}(A)$ corresponds to a ring homomorphism $f^{\#} : A \to B$. Let $s \in A$. By definition of morphism of schemes, we have that $f^{-1}(\mathrm{D}(s)) = \mathrm{D}(f^{\#}(s)) = \mathrm{Spec}(B_{f^{\#}(s)})$. So $\mathrm{Spec}(A_s) = \mathrm{D}(s)$ has affine preimage.
On the other hand, let $U = \mathrm{Spec}(A)$ be an open affine subset of X and let $(s_i)_{i\in I}$ be a collection of elements of A such that $\sum_{i\in I} s_i A = A$ and $f^{-1}(\mathrm{D}(s_i))$ is affine for every $i \in I$. Define $B := \mathcal{O}_Y(f^{-1}(U)) = \mathcal{O}_{f^{-1}(U)}(f^{-1}(U))$. The morphism of schemes f induces a ring homomorphism $f^{\#} : \mathcal{O}_X(U) = \mathcal{O}_{\mathrm{Spec}(A)}(\mathrm{Spec}(A)) = A \to \mathcal{O}_Y(f^{-1}(U)) = B$. Since $\sum_{i\in I} s_i A = A$, there exist $\lambda_i \in A$ (for every $i \in I$) such that $1_A = \sum_{i\in I} s_i\lambda_i$. Then, since $f^{\#}$ is a ring homomorphism, we have that

$$1_B = f^{\#}(1_A) = f^{\#}\left(\sum_{i\in I} s_i\lambda_i\right) = \sum_{i\in I} f^{\#}(s_i)f^{\#}(s_i) \in \sum_{i\in I} f^{\#}(s_i)B\ .$$

Since $\sum_{i\in I} f^{\#}(s_i)B$ is an ideal of B, this implies that $\sum_{i\in I} f^{\#}(s_i)B = B$. Moreover, let $i \in I$. Recalling that $\mathrm{D}(s_i) = \mathrm{Spec}(A)_{s_i}$ (see remark 2.2.8 or the proof of lemma 2.2.7(3)), we have that

$$\begin{aligned} f^{-1}(\mathrm{D}(s_i)) = \{y \in Y \mid f(y) \in \mathrm{D}(s_i) = \mathrm{Spec}(A)_{s_i}\} = \\ = \{y \in f^{-1}(U) \mid (s_i)_{f(y)} \notin \mathfrak{m}_{\mathrm{Spec}(A),f(y)}\} = \\ = \{y \in f^{-1}(U) \mid (f^{\#}(s_i))_y \notin \mathfrak{m}_{f^{-1}(U),y}\} = f^{-1}(U)_{f^{\#}(s_i)} , \end{aligned}$$

by definition of morphism of schemes. So $f^{-1}(U)_{f^{\#}(s_i)}$ is affine. Then $f^{-1}(U)$ satisfies the assumptions of lemma 2.2.9. This allows us to conclude that $f^{-1}(U)$ is affine. By the affine communication lemma, we get the claim.

(2) If for every open affine subscheme $U = \mathrm{Spec}(A)$ of X the open subscheme $f^{-1}(U)$ of Y is affine and equal to $\mathrm{Spec}(B)$, where the A-algebra B is finitely generated as an A-module, then every cover of X by open affine subsets satisfies the condition required in the definition and such a cover exists by definition of scheme. So f is finite.
Conversely, assume that f is finite. Then there exists a cover of X by open affine subsets $(U_i = \mathrm{Spec}(A_i))_{i\in I}$ such that, for any $i \in I$, $f^{-1}(U_i)$ is affine and equal to $\mathrm{Spec}(B_i)$, where the A_i-algebra B_i is finitely generated as an A_i-module. We want to prove that the property "$f^{-1}(\mathrm{Spec}(A)) = \mathrm{Spec}(B)$ with B finitely generated as an A-module" satisfies the assumptions of the affine communication lemma. Let $U = \mathrm{Spec}(A)$ be an open affine subscheme of X such that $f^{-1}(U)$ is affine and $f^{-1}(U) = \mathrm{Spec}(B)$, where the A-algebra B is finitely generated as an A-module. The morphism $f : f^{-1}(U) = \mathrm{Spec}(B) \to U = \mathrm{Spec}(A)$ corresponds to a ring homomorphism $f^{\#} : A \to B$. Let $s \in A$ and consider $\mathrm{D}(s) = \mathrm{Spec}(A_s)$. As above, we have that $f^{-1}(\mathrm{D}(s)) = \mathrm{D}(f^{\#}(s)) = \mathrm{Spec}(B_{f^{\#}(s)})$ is affine. Moreover, if $(w_1, \ldots, w_n)$ generates B over A, then $\left(\frac{w_1}{1}, \ldots, \frac{w_n}{1}\right)$ generates $B_{f^{\#}(s)}$ over A_s (notice that $B_{f^{\#}(s)} \cong B_s$ as an A_s-module). So $B_{f^{\#}(s)}$ is finitely generated as an A_s-module.
On the other hand, let $U = \mathrm{Spec}(A)$ be an open affine subset of X and let $(s_i)_{i\in I}$ be a collection of elements of A such that $\sum_{i\in I} s_i A = A$ and, for every $i \in I$, $f^{-1}(\mathrm{D}(s_i))$ is affine and equal to $\mathrm{Spec}(B_i)$, where the A_{s_i}-algebra B_i is finitely generated as an A_{s_i}-module. Since f is finite, it is in particular affine. So, by point (1), we have that $f^{-1}(U)$ is affine, i.e. there exists a ring B such that $f^{-1}(U) = \mathrm{Spec}(B)$. Then for every $i \in I$ we have that $\mathrm{Spec}(B_i) = f^{-1}(\mathrm{D}(s_i)) = \mathrm{D}(f^{\#}(s_i)) = \mathrm{Spec}(B_{f^{\#}(s_i)})$. Then $B_i \cong B_{f^{\#}(s_i)} \cong B_{s_i}$ as an A_{s_i}-module. So B_{s_i} is finitely generated as an A_{s_i}-module for any $i \in I$. By lemma 2.1.29(3), B is finitely generated as an A-module. By the affine communication lemma, we get the claim.

(3) Assume that for every open affine subscheme $U = \mathrm{Spec}(A)$ of X the open subscheme $f^{-1}(U)$ of Y is affine and equal to $\mathrm{Spec}(B)$, where B is a finite projective A-algebra. By definition of scheme, there exists a cover of X by open affine subsets $(U_i = \mathrm{Spec}(A_i))_{i\in I}$. By assumption, for every $i \in I$ we have $f^{-1}(U_i) = \mathrm{Spec}(B_i)$, where B_i is a finite projective A_i-algebra. Fix $i \in I$. By proposition 2.1.30 ((i) $\Longrightarrow$ (iv)), there exists a collection $(s_{ij})_{j\in J_i}$ of elements of A_i such that $\sum_{j\in J_i} s_{ij} A_i = A_i$ and for each $j \in J_i$ we have that

$(B_i)_{s_{ij}}$ is a free $(A_i)_{s_{ij}}$-module of finite rank. Define now $U_{ij} = \mathrm{Spec}((A_i)_{s_{ij}}) = \mathrm{D}(s_{ij}) \subseteq \mathrm{Spec}(A_i) = U_i$, for every $i \in I$, $j \in J_i$. Then U_{ij} is an open affine subset of X for any $i \in I$, $j \in J_i$. Moreover, if $\mathfrak{p} \in \mathrm{Spec}(A_i)$ then there exists $j \in J_i$ such that $s_{ij} \notin \mathfrak{p}$ (otherwise we would have $A_i = \sum_{j\in J_i} s_{ij}A_i \subseteq \mathfrak{p}$, which is a contradiction because any prime ideal is a proper ideal). This means that $\mathfrak{p} \in \mathrm{D}(f_{ij}) = U_{ij}$. So $U_i = \bigcup_{j\in J_i} U_{ij}$, for any $i \in I$. Then $X = \bigcup_{i\in I} U_i = \bigcup_{i\in I}\bigcup_{j\in J_i} U_{ij}$, i.e. $(U_{ij})_{i\in I, j\in J_i}$ is a cover of X by open affine subsets. Let $i \in I$, $j \in J_i$. The morphism $f : f^{-1}(U_i) = \mathrm{Spec}(B_i) \to U_i = \mathrm{Spec}(A_i)$ corresponds to a ring homomorphism $f^{\#} : A_i \to B_i$. As above, we have that $f^{-1}(U_{ij}) = f^{-1}(\mathrm{D}(s_{ij})) = \mathrm{D}(f^{\#}(s_{ij})) = \mathrm{Spec}((B_i)_{f^{\#}(s_{ij})})$. But $(B_i)_{f^{\#}(s_{ij})} \cong (B_i)_{s_{ij}}$ is finitely generated and free as an $(A_i)_{s_{ij}}$-module. So f is finite and locally free.
Conversely, assume that f is finite and locally free. Then there exists a cover of X by open affine subsets $(U_i = \mathrm{Spec}(A_i))_{i\in I}$ such that, for any $i \in I$, $f^{-1}(U_i)$ is affine and equal to $\mathrm{Spec}(B_i)$, where the A_i-algebra B_i is finitely generated and free as an A_i-module. In particular, B_i is finitely generated and projective as an A_i-module, i.e. it is a finite projective A_i-algebra. We want to prove that the property "$f^{-1}(\mathrm{Spec}(A)) = \mathrm{Spec}(B)$ with B a finite projective A-algebra" satisfies the assumptions of the affine communication lemma. Let $U = \mathrm{Spec}(A)$ be an open affine subscheme of X such that $f^{-1}(U)$ is affine and $f^{-1}(U) = \mathrm{Spec}(B)$, where B is a finite projective A-algebra. The morphism $f : f^{-1}(U) = \mathrm{Spec}(B) \to U = \mathrm{Spec}(A)$ corresponds to a ring homomorphism $f^{\#} : A \to B$. Let $s \in A$ and consider $\mathrm{D}(s) = \mathrm{Spec}(A_s)$. As above, we have that $f^{-1}(\mathrm{D}(s)) = \mathrm{D}(f^{\#}(s)) = \mathrm{Spec}(B_{f^{\#}(s)})$ is affine and $B_{f^{\#}(s)}$ is finitely generated as an A_s-module, because B is finitely generated over A. Moreover, $B_{f^{\#}(s)} \cong B_s \cong B \otimes_A A_s$ is projective as an A_s-module by lemma 2.1.24. So $B_{f^{\#}(s)}$ is a finite projective A_s-algebra.
On the other hand, let $U = \mathrm{Spec}(A)$ be an open affine subset of X and let $(s_i)_{i\in I}$ be a collection of elements of A such that $\sum_{i\in I} s_iA = A$ and, for every $i \in I$, $f^{-1}(\mathrm{D}(s_i))$ is affine and equal to $\mathrm{Spec}(B_i)$, where B_i is a finite projective A_{s_i}-algebra. Since f is finite and locally free, it is in particular affine. So, by point (1), we have that $f^{-1}(U)$ is affine, i.e. there exists a ring B such that $f^{-1}(U) = \mathrm{Spec}(B)$. Then for every $i \in I$ we have that $\mathrm{Spec}(B_i) = f^{-1}(\mathrm{D}(s_i)) = \mathrm{D}(f^{\#}(s_i)) = \mathrm{Spec}(B_{f^{\#}(s_i)})$. Fix $i \in I$. Then $B_i \cong B_{f^{\#}(s_i)} \cong B_{s_i}$ as an A_{s_i}-module. So B_{s_i} is a finite projective A_{s_i}-algebra, i.e. it is finitely generated and projective as an A_{s_i}-module. Since this holds for every $i \in I$, by corollary 2.1.32 we have that B is finitely generated and projective as an A-module, i.e. B is a finite projective A-algebra. By the affine communication lemma, we get the claim.

(4) Assume that for every open affine subscheme $U = \mathrm{Spec}(A)$ of X the open subscheme $f^{-1}(U)$ of Y is affine and equal to $\mathrm{Spec}(B)$, where B is a projective separable A-algebra. Since any projective separable A-algebra is a finite projective A-algebra, we can apply point (3) to get that f is finite and locally free. So there exists a cover of X by open affine subsets $(U_i = \mathrm{Spec}(A_i))_{i\in I}$ such that, for every $i \in I$, $f^{-1}(U_i)$ is affine and equal to $\mathrm{Spec}(B_i)$, where the

A_i-algebra B_i is finitely generated and free as an A_i-module. By assumption we have also that B_i is a projective separable A_i-algebra. Combining the two things, we get that B_i is a free separable A_i-algebra for every $i \in I$ (see remark 2.1.61). So f is finite étale.
Conversely, assume that f is finite étale. Then there exists a cover of X by open affine subsets $(U_i = \mathrm{Spec}(A_i))_{i\in I}$ such that, for any $i \in I$, $f^{-1}(U_i)$ is affine and equal to $\mathrm{Spec}(B_i)$, where B_i is a free separable A_i-algebra. In particular, B_i is a projective separable A_i-algebra. We want to prove that the property "$f^{-1}(\mathrm{Spec}(A)) = \mathrm{Spec}(B)$ with B a projective separable A-algebra" satisfies the assumptions of the affine communication lemma. Let $U = \mathrm{Spec}(A)$ be an open affine subscheme of X such that $f^{-1}(U)$ is affine and $f^{-1}(U) = \mathrm{Spec}(B)$, where B is a projective separable A-algebra. The morphism $f : f^{-1}(U) = \mathrm{Spec}(B) \to U = \mathrm{Spec}(A)$ corresponds to a ring homomorphism $f^\# : A \to B$. Let $s \in A$ and consider $\mathrm{D}(s) = \mathrm{Spec}(A_s)$. As above, we have that $f^{-1}(\mathrm{D}(s)) = \mathrm{D}(f^\#(s)) = \mathrm{Spec}(B_{f^\#(s)})$ is affine. Moreover, $B_{f^\#(s)} \cong B_s \cong B \otimes_A A_s$ is a projective separable A_s-algebra by lemma 2.1.71.
On the other hand, let $U = \mathrm{Spec}(A)$ be an open affine subset of X and let $(s_i)_{i\in I}$ be a collection of elements of A such that $\sum_{i\in I} s_i A = A$ and, for every $i \in I$, $f^{-1}(\mathrm{D}(s_i))$ is affine and equal to $\mathrm{Spec}(B_i)$, where B_i is a projective separable A_{s_i}-algebra. Since f is finite étale, it is in particular affine. So, by point (1), we have that $f^{-1}(U)$ is affine, i.e. there exists a ring B such that $f^{-1}(U) = \mathrm{Spec}(B)$. Then for every $i \in I$ we have that $\mathrm{Spec}(B_i) = f^{-1}(\mathrm{D}(s_i)) = \mathrm{D}(f^\#(s_i)) = \mathrm{Spec}(B_{f^\#(s_i)})$. Fix $i \in I$. Then $B_i \cong B_{f^\#(s_i)} \cong B_{s_i}$ as an A_{s_i}-module. So B_{s_i} is a projective separable A_{s_i}-algebra. Since this holds for every $i \in I$, by proposition 2.1.73 we have that B is a projective separable A-algebra. By the affine communication lemma, we get the claim.

□

Remark 2.2.11. It is now clear why we had to introduce the notion of projective algebras: the properties "$f^{-1}(\mathrm{Spec}(A)) = \mathrm{Spec}(B)$ with B finitely generated and free as an A-module" and "$f^{-1}(\mathrm{Spec}(A)) = \mathrm{Spec}(B)$ with B a free separable A-algebra" do not satisfy the assumptions of the communication lemma (more precisely, the second assumption). Then the notion of free separable algebras would not be enough to give a complete affine description of finite étale morphisms.

Lemma 2.2.12. *Let X, Y be schemes and $f : Y \to X$ a finite and locally free morphism of schemes. For any open affine subscheme $U = \mathrm{Spec}(A)$ of X, define $d_U := [B : A] : U = \mathrm{Spec}(A) \to \mathbb{Z}$ (see the definitions 2.1.51 and 2.1.35), where B is the finite projective A-algebra such that $f^{-1}(U) = \mathrm{Spec}(B)$ (lemma 2.2.10(3)). Then there exists a locally constant function $d : \mathrm{sp}(X) \to \mathbb{Z}$ (where $\mathrm{sp}(X)$ denotes the underlying topological space of X) such that $d_{|_U} = d_U$ for every open affine subscheme U of X. In particular, d is continuous (considering the discrete topology on $\mathbb{Z}$) and it is constant if X is connected.*

Proof. We have that d_U is locally constant for every open affine subscheme $U =$

Spec(A), by corollary 2.1.33(2). Then, since open affine subsets cover X (by definition of scheme), it is enough to show that the the d_U's agree on the overlaps. Let $U_1 = \mathrm{Spec}(A_1)$ and $U_2 = \mathrm{Spec}(A_2)$ be two open affine subschemes of X, with $f^{-1}(U_1) = \mathrm{Spec}(B_1)$ and $f^{-1}(U_2) = \mathrm{Spec}(B_2)$ (B_1 and B_2 finite projective algebras over A_1 and A_2, respectively). Let $\mathfrak{p} \in U_1 \cap U_2$. By lemma 2.2.5, there exists $W \subseteq U \cap V$ such that $\mathfrak{p} \in W$ and $W = \mathrm{D}(s) = \mathrm{D}(t)$ for some $s \in A_1$, $t \in A_2$. Then $s \notin \mathfrak{p}$ and $t \notin \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this implies $s^n, t^n \notin \mathfrak{p}$ for any $n \in \mathbb{N}$, i.e. $S_s \subseteq A_1 \backslash \mathfrak{p}$ and $S_t \subseteq A_2 \backslash \mathfrak{p}$. We have that $W = \mathrm{Spec}((A_1)_s) = \mathrm{Spec}((A_2)_t)$ is affine. We identify $\mathfrak{p}$ with $\mathfrak{p}_s \in \mathrm{Spec}((A_1)_s)$ and $\mathfrak{p}_t \in \mathrm{Spec}((A_2)_t)$. Let $f_1^{\#} : \mathcal{O}_X(U_1) = \mathcal{O}_{\mathrm{Spec}(A_1)}(\mathrm{Spec}(A_1)) = A_1 \to \mathcal{O}_Y(f^{-1}(U_1)) = \mathcal{O}_{\mathrm{Spec}(B_1)}(\mathrm{Spec}(B_1)) = B_1$ be the ring homomorphism induced by f. We have that $f^{-1}(W) = f^{-1}(\mathrm{D}(s)) = \mathrm{D}(f_1^{\#}(s)) = \mathrm{Spec}\left((B_1)_{f_1^{\#}(s)}\right)$. Then

$$d_W(\mathfrak{p}) = [(B_1)_{f_1^{\#}(s)} : (A_1)_s](\mathfrak{p}_s) = \mathrm{rank}_{((A_1)_s)_{\mathfrak{p}_s}}\left(\left((B_1)_{f_1^{\#}(s)}\right)_{\mathfrak{p}_s}\right) .$$

We have that $(B_1)_{f_1^{\#}(s)} \cong (B_1)_s$ as an $(A_1)_s$-module. So $\left((B_1)_{f_1^{\#}(s)}\right)_{\mathfrak{p}_s} \cong ((B_1)_s)_{\mathfrak{p}_s}$ as $((A_1)_s)_{\mathfrak{p}_s}$-modules. We have also that $((A_1)_s)_{\mathfrak{p}_s} \cong (A_1)_{\mathfrak{p}}$. This isomorphism allows us to see $\left((B_1)_{f_1^{\#}(s)}\right)_{\mathfrak{p}_s} \cong ((B_1)_s)_{\mathfrak{p}_s}$ as as an $(A_1)_{\mathfrak{p}}$-module (free of the same rank). Then $((B_1)_s)_{\mathfrak{p}_s} \cong (B_1)_{\mathfrak{p}}$ as $(A_1)_{\mathfrak{p}}$-modules and so

$$d_W(\mathfrak{p}) = \mathrm{rank}_{((A_1)_s)_{\mathfrak{p}_s}}\left(\left((B_1)_{f_1^{\#}(s)}\right)_{\mathfrak{p}_s}\right) = \mathrm{rank}_{(A_1)_{\mathfrak{p}}}((B_1)_{\mathfrak{p}}) = [B_1 : A_1](\mathfrak{p}) = d_{U_1}(\mathfrak{p}) .$$

Analogously, one can prove that $d_W(\mathfrak{p}) = d_{U_2}(\mathfrak{p})$. Then $d_{U_1}(\mathfrak{p}) = d_{U_2}(\mathfrak{p})$. Since this holds for every $\mathfrak{p} \in U_1 \cap U_2$, we get that $(d_{U_1})_{|U_1 \cap U_2} = (d_{U_2})_{|U_1 \cap U_2}$. □

Remark 2.2.13. Let X, Y be schemes and $f : Y \to X$ a finite and locally free morphism of schemes. Consider the pushforward $f_*\mathcal{O}_Y$, which is a sheaf of $\mathcal{O}_X$-algebras. Applying remark 2.1.31 to any open affine subscheme, one gets that $f_*\mathcal{O}_Y$ is locally free of finite rank as an $\mathcal{O}_X$-module. Then the function d defined in 2.2.12 could also be obtained by working on stalks, as in 2.1.34. However, notice that these stalks are not stalks of $\mathcal{O}_Y$.

Definition 2.2.14. Let X, Y be schemes and $f : Y \to X$ a finite and locally free morphism of schemes. We denote the function d defined in 2.2.12 by $[Y : X]$ or $\deg(f)$ and we call it the *degree of* Y *over* X or the *degree of* f.

The following lemma illustrates the importance of the degree of a finite and locally free morphism.

Lemma 2.2.15. *Let X, Y be two schemes and $f : Y \to X$ a finite and locally free morphism of schemes. Then:*

(1) $Y = \emptyset$ if and only if $[Y : X] = 0$ (i.e. $[Y : X](x) = 0$ for any $x \in X$);

(2) f is an isomorphism if and only if $[Y : X] = 1$ (i.e. $[Y : X](x) = 1$ for any $x \in X$);

(3) *f is surjective if and only if $[Y : X] \geq 1$ (i.e. $[Y : X](x) \geq 1$ for any $x \in X$), and if and only if for every open affine subset $U = \mathrm{Spec}(A)$ of X we have $f^{-1}(U) = \mathrm{Spec}(B)$, where B is a faithfully projective A-algebra.*

Proof. Recall that for every open affine subset U of X the preimage $f^{-1}(U)$ is affine and equal to $\mathrm{Spec}(B)$, with B a finite projective A-algebra (lemma 2.2.10(3)). Moreover, for every open affine subset U of X, let d_U be defined as in lemma 2.2.12.

(1) If $Y = \emptyset$, then $f^{-1}(U) = \emptyset = \mathrm{Spec}(0)$ for every open affine subset $U = \mathrm{Spec}(A)$ of X, which implies that $d_U = [0 : A] = 0$. So $[Y : X] = 0$.
Conversely, assume that $[Y : X] = 0$. Let $U = \mathrm{Spec}(A)$ be an open affine subset of X, with $f^{-1}(U) = \mathrm{Spec}(B)$ (B a finite projective A-algebra). Then $[B : A] = d_U = [Y : X]_{|U} = 0$, which means that for every prime ideal $\mathfrak{p}$ of A we have $\mathrm{rank}_{A_\mathfrak{p}}(B_\mathfrak{p}) = 0$, i.e. $B_\mathfrak{p} = 0$. By lemma 2.1.28(1), this implies that $B = 0$. So $f^{-1}(U) = \mathrm{Spec}(0) = \emptyset$. By definition of scheme, X is covered by its open affine subsets. Then

$$Y = f^{-1}(X) = f^{-1}\left(\bigcup_{\substack{U\subseteq X\\ \text{open affine}}} U\right) = \bigcup_{\substack{U\subseteq X\\ \text{open affine}}} f^{-1}(U) = \bigcup_{\substack{U\subseteq X\\ \text{open affine}}} \emptyset = \emptyset\,.$$

(2) Assume that f is an isomorphism. Then for every open affine subset $U = \mathrm{Spec}(A)$ of X we have that $f^{-1}(U) \cong U = \mathrm{Spec}(A)$ and $d_U = [A : A] = 1$. So $[Y : X] = 1$.
Conversely, assume that $[Y : X] = 1$. Let $U = \mathrm{Spec}(A)$ be an open affine subset of X, with $f^{-1}(U) = \mathrm{Spec}(B)$ (B a finite projective A-algebra). Then $[B : A] = d_U = [Y : X]_{|U} = 1$. By lemma 2.1.58(3), this implies that the ring homomorphism $f^{\#} : A \to B$ induced by $f : f^{-1}(U) = \mathrm{Spec}(B) \to U = \mathrm{Spec}(A)$ (i.e. the ring homomorphism which defines the A-algebra structure on B, see remark 2.2.2(1)) is an isomorphism. Since the correspondence between morphism of schemes $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ and ring homomorphism $A \to B$ is bijective and preserves compositions, it follows that $f : f^{-1}(U) \to U$ is an isomorphism of schemes. Then it has an inverse $g_U := \left(f_{|f^{-1}(U)}\right)^{-1} : U \to f^{-1}(U)$. The morphisms g_U's are compatible with each other. Indeed, if U, V are two open affine subsets of X, we have that

$$\begin{aligned}(g_U)_{|U\cap V} &= \left(\left(f_{|f^{-1}(U)}\right)^{-1}\right)_{|U\cap V} = \\ &= \left(\left(f_{|f^{-1}(U)}\right)_{|f^{-1}(U)\cap f^{-1}(V)}\right)^{-1} = \left(f_{|f^{-1}(U)\cap f^{-1}(V)}\right)^{-1} = \\ &= \left(\left(f_{|f^{-1}(V)}\right)_{|f^{-1}(U)\cap f^{-1}(V)}\right)^{-1} = \left(\left(f_{|f^{-1}(V)}\right)^{-1}\right)_{|U\cap V} = (g_V)_{|U\cap V}\,.\end{aligned}$$

Then, since X is covered by its open affine subsets, we can glue the g_U's and get a morphism of schemes $g : X \to Y$. We have that g and f are inverse to each other, because this is true considering the restrictions to U and $f^{-1}(U)$, for every open affine subset U of X. So f is an isomorphism.

(3) First of all, notice that $[Y : X] \geq 1$ if and only if for every open affine subset $U = \mathrm{Spec}(A)$ we have that $[B : A] = d_U \geq 1$, i.e. B is faithfully projective, by definition (2.1.51(2)), where B is the finite projective A-algebra such that $f^{-1}(U) = \mathrm{Spec}(B)$. So the last part of the statement is obvious.
Since X is covered by its open affine subsets, we have that f is surjective if and only if $f : f^{-1}(U) \to U$ is surjective for every open affine subset U of X. On the other hand, $[Y : X] \geq 1$ if and only if $d_U \geq 1$ for every open affine subset U of X. Then it is enough to prove that, for any open affine subset U of X, $f : f^{-1}(U) \to U$ is surjective if and only if $d_U \geq 1$.
Let $U = \mathrm{Spec}(A)$ be an open affine subset of X, with $f^{-1}(U) = \mathrm{Spec}(B)$, where B is a finite projective A-algebra. Let $f^{\#} : A \to B$ be the ring homomorphism that corresponds to $f : f^{-1}(U) = \mathrm{Spec}(B) \to U = \mathrm{Spec}(A)$. Assume that $f : f^{-1}(U) = \mathrm{Spec}(B) \to U = \mathrm{Spec}(A)$ is surjective. Let $\mathfrak{p} \in \mathrm{Spec}(A)$. Then there exists $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{p} = f(\mathfrak{q}) = (f^{\#})^{-1}(\mathfrak{q})$. If $s \in A \backslash \mathfrak{p}$, then $f^{\#}(s) \in B \backslash \mathfrak{q}$. So we can consider the following map:

$$\varphi : B_{\mathfrak{p}} \to B_{\mathfrak{q}}, \ \frac{x}{s} \mapsto \frac{x}{f^{\#}(s)} \ .$$

Let $x_1, x_2 \in B$, $s_1, s_2 \in A \backslash \mathfrak{p}$ such that $\frac{x_1}{s_1} = \frac{x_2}{s_2}$. This means that there exists $u \in A \backslash \mathfrak{p}$ such that $u(s_2 x_1 - s_1 x_2) = 0$. By definition of the A-module structure on B, we have that $u(s_2 x_1 - s_1 x_2) = f^{\#}(u)(f^{\#}(s_1)x_1 - f^{\#}(s_2)x_2)$. So $f^{\#}(u)(f^{\#}(s_1)x_1 - f^{\#}(s_2)x_2) = 0$, which implies that $\frac{x_1}{f^{\#}(s_1)} = \frac{x_2}{f^{\#}(s_2)}$, because $f^{\#}(u) \in B \backslash \mathfrak{q}$. So φ is well defined. We have that $\varphi\left(\frac{1}{1}\right) = \frac{1}{f^{\#}(1)} = \frac{1}{1}$ and $\varphi\left(\frac{0}{1}\right) = \frac{0}{f^{\#}(1)} = \frac{0}{1}$ (actually, it is easy to prove that φ is an A-linear ring homomorphism). If we had $\frac{1}{1} = \frac{0}{1}$ in $B_{\mathfrak{q}}$, there would exist $t \in B \backslash \mathfrak{q}$ such that $0 = t \cdot 1 = t$, but this is a contradiction because $0 \in \mathfrak{q}$. So $\frac{1}{1} \neq \frac{0}{1}$ in $B_{\mathfrak{p}}$, which implies that $B_{\mathfrak{p}} \neq 0$. Then $d_U(\mathfrak{p}) = [B : A](\mathfrak{p}) = \mathrm{rank}_{A_{\mathfrak{p}}}(B_{\mathfrak{p}}) \geq 1$.
Conversely, assume that $[B : A] = d_U \geq 1$. By lemma 2.1.58(1), this implies that $f^{\#} : A \to B$ is injective. So we can assume that $A \subseteq B$, identifying A with $f^{\#}(A)$. Since B is finitely generated as an A-module, we have that B is integral over A. Then, by the "lying-over" theorem ([3], theorem 5.10), for every $\mathfrak{p} \in \mathrm{Spec}(A)$ there exists $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{p} = \mathfrak{q} \cap A = f(\mathfrak{q})$. This shows that $f : \mathrm{Spec}(B) = f^{-1}(U) \to \mathrm{Spec}(A) = U$ is surjective.

□

Remark 2.2.16. We can associate a degree function also to any finite covering of topological spaces (see remark 1.2(2) in the appendix). The lemma we have just proved corresponds to a result that is obvious in the case of topological spaces. Namely, given a finite covering $f : Y \to X$, with X, Y two topological spaces, we have that:

(1) $Y = \emptyset$ if and only if $|f^{-1}(x)| = 0$ for every $x \in X$;

(2) f is a homeomorphism if and only if $|f^{-1}(x)| = 1$ for every $x \in X$ (for an arbitrary map this would mean that the map is bijective: the fact that the inverse is also continuous follows from the definition of covering);

(3) f is surjective if and only if $|f^{-1}(x)| \geq 1$ for every $x \in X$.

Corollary 2.2.17. *Let X, Y be two schemes and $f : Y \to X$ a morphism of schemes. We have that f is surjective, finite and locally free if and only if for every open affine subscheme $U = \operatorname{Spec}(A)$ of X the open subscheme $f^{-1}(U)$ of Y is affine and equal to $\operatorname{Spec}(B)$, where B is a faithfully projective A-algebra.*

Proof. If f is surjective, finite and locally free, then the claim follows directly from lemma 2.2.15(3).
Conversely, assume that for every open affine subscheme $U = \operatorname{Spec}(A)$ of X the open subscheme $f^{-1}(U)$ of Y is affine and equal to $\operatorname{Spec}(B)$, where B is a faithfully projective A-algebra. Since any faithfully projective A-algebra is in particular a finite projective A-algebra, by lemma 2.2.10(3) we have that f is finite and locally free. Then we can apply lemma 2.2.15(3) to get that f is also surjective. □

We list now some properties of finite and locally free morphisms and of finite étale morphisms. Particularly important is the fact that base changes preserve finite étale morphisms (lemma 2.2.28(4)).

Lemma 2.2.18. *Let X, $Y_1, \dots, Y_n$ be schemes ($n \in \mathbb{N}$) with morphisms $f_i : Y_i \to X$ for every $i = 1, \dots, n$. Define $Y := \coprod_{i=1}^n Y_i$ (disjoint union of schemes) and consider the morphism $f : Y \to X$ obtained by gluing the f_i's. We have that:*

(1) f is finite and locally free if and only if f_i is finite and locally free for every $i = 1, \dots, n$;

(2) if f is finite and locally free, then $[Y : X] = \sum_{i=1}^n [Y_i : X]$ (as functions on X);

(3) f is finite étale if and only if f_i is finite étale for every $i = 1, \dots, n$.

Proof. (1) Assume that f_i is finite and locally free for every $i = 1, \dots, n$. Let $U = \operatorname{Spec}(A)$ be an open affine subset of X. By lemma 2.2.10(3), for every $i = 1, \dots, n$ we have that $f_i^{-1}(U)$ is affine and equal to $\operatorname{Spec}(B_i)$, where B_i is a finite projective A-algebra. By definition of f, we have that $f^{-1}(U) = \coprod_{i=1}^n f_i^{-1}(U) = \coprod_{i=1}^n \operatorname{Spec}(B_i)$. Define $B := \mathcal{O}_Y(f^{-1}(U)) = \mathcal{O}_{f^{-1}(U)}(f^{-1}(U))$. By definition of sheaf, we have that $B = \mathcal{O}_Y(f^{-1}(U)) \cong \prod_{i=1}^n \mathcal{O}_Y(f_i^{-1}(U)) = \prod_{i=1}^n \mathcal{O}_{\operatorname{Spec}(B_i)}(\operatorname{Spec}(B_i)) = \prod_{i \in I} B_i$. Notice that this is an isomorphism of A-algebras, because for every $i \in I$ the commutativity of the diagram

$$\begin{array}{ccc} f_i^{-1}(U) & \hookrightarrow & f^{-1}(U) \\ & \searrow^{f_i} & \downarrow f \\ & & U \end{array}$$

implies the commutativity of the corresponding diagram of ring homomorphisms. For every $i \in I$, let s_i be the unique element of $B = \mathcal{O}_Y(f^{-1}(U))$ such that $\rho_{f^{-1}(U),f_j^{-1}(U)}(s_i) = \delta_{ij}$ for any $j \in I$. Consider the sum $\sum_{i\in I} s_i$. For every $j \in I$ we have that

$$\rho_{f^{-1}(U),f_j^{-1}(U)}\left(\sum_{i\in I} s_i\right) = \sum_{i\in I} \rho_{f^{-1}(U),f_j^{-1}(U)}(s_i) = \\ = \sum_{i\in I} \delta_{ij} = 1 = \rho_{f^{-1}(U),f_j^{-1}(U)}(1)$$

(because $\rho_{f^{-1}(U),f_j^{-1}(U)}$ is a ring homomorphism). By definition of sheaf, this implies that $1 = \sum_{i\in I} s_i \in \sum_{i\in I} s_i A$. Since $\sum_{i\in I} s_i A$ is an ideal of A, it follows that $\sum_{i\in I} s_i A = A$. Moreover, we have that

$$(f^{-1}(U))_{s_j} = \{y \in f^{-1}(U) \mid (s_j)_y \notin \mathfrak{m}_{f^{-1}(U),y}\} = \\ = \coprod_{i\in I} \left\{ y \in f_i^{-1}(U) \;\middle|\; (\delta_{ij})_y = (\rho_{f^{-1}(U),f_i^{-1}(U)}(s_j))_y \notin \mathfrak{m}_{f^{-1}(U),y} \right\} = f_j^{-1}(U)$$

is affine for every $j \in I$. By lemma 2.2.9, it follows that $f^{-1}(U)$ is affine and isomorphic to $\mathrm{Spec}(B)$. Since $B \cong \prod_{i=1}^n B_i$ and B_i is a finite projective A-algebra for every $i \in I$, by lemma 2.1.52 we have that B is a finite projective A-algebra. Since this holds for every open affine subset $U = \mathrm{Spec}(A)$ of X, by lemma 2.2.10(3) we have that f is finite and locally free.
Conversely, assume that f is finite and locally free. Let $U = \mathrm{Spec}(A)$ be an open affine subset of X. By lemma 2.2.10(3), we have that $f^{-1}(U)$ is affine and equal to $\mathrm{Spec}(B)$, where B is a finite projective A-algebra. By definition of f, we have that $\mathrm{Spec}(B) = f^{-1}(U) = \coprod_{i=1}^n f_i^{-1}(U)$. Then, by definition of sheaf, we have that $B = \mathcal{O}_{\mathrm{Spec}(B)}(\mathrm{Spec}(B)) = \mathcal{O}_Y(f^{-1}(U)) \cong \prod_{i=1}^n \mathcal{O}_Y(f_i^{-1}(U))$ (as above, this is an isomorphism of A-algebras). Fix $i \in I$ and let s_i be the unique element of $B = \mathcal{O}_Y(f^{-1}(U))$ such that $\rho_{f^{-1}(U),f_j^{-1}(U)}(s_i) = \delta_{ij}$ for any $j \in I$. As above, we have that $f_i^{-1}(U) = (f^{-1}(U))_{s_i}$. But, as in remark 2.2.8 (see also the proof of lemma 2.2.7(3)), we have that $(f^{-1}(U))_{s_i} = (\mathrm{Spec}(B))_{s_i} = \mathrm{D}(s_i)$. So $f_i^{-1}(U) = \mathrm{D}(s_i) = \mathrm{Spec}(B_{s_i})$ is affine. Moreover, we have that $B \cong \prod_{i=1}^n \mathcal{O}_Y(f_i^{-1}(U)) = \prod_{i=1}^n \mathcal{O}_{\mathrm{Spec}(B_{s_i})}(\mathrm{Spec}(B_{s_i})) = \prod_{i=1}^n B_{s_i}$ as A-algebras. Since B is a finite projective A-algebra, by lemma 2.1.52 we have that B_{s_i} is a finite projective A-algebra for every $i = 1, \ldots, n$. Since this holds for every open affine subset $U = \mathrm{Spec}(A)$ of X, by lemma 2.2.10(3) we have that f_i is finite and locally free for every $i = 1, \ldots, n$.

(2) Let $U = \mathrm{Spec}(A)$ be an open affine subset of X. As in the proof of point (1), we can write $f^{-1}(U) = \mathrm{Spec}(B)$ and $f^{-1}(U) = \mathrm{Spec}(B_i)$ for every $i = 1, \ldots, n$, with $B, B_1, \ldots, B_n$ finite projective A-algebras and $B \cong \prod_{i=1}^n B_i$ as A-algebras. This means that $B \cong \bigoplus_{i=1}^n B_i$ as A-modules. Let d_U be defined as in lemma 2.2.12 and let $d_U^{(i)}$ be defined in the same way but considering f_i instead of f, for every $i = 1, \ldots, n$. By lemma 2.1.37, we have that

$$d_U = [B : A] = \mathrm{rank}_A(B) = \sum_{i=1}^n \mathrm{rank}_A(B_i) = \sum_{i=1}^n [B_i : A] = \sum_{i=1}^n d_U^{(i)} .$$

Since this holds for any open affine subset U of X, we get that $[Y : X] = \sum_{i=1}^{n}[Y_i : X]$.

(3) Assume that f_i is finite étale for every $i = 1, \dots, n$. Let $U = \mathrm{Spec}(A)$ be an open affine subset of X. By lemma 2.2.10(4), for every $i = 1, \dots, n$ we have that $f_i^{-1}(U)$ is affine and equal to $\mathrm{Spec}(B_i)$, where B_i is a projective separable A-algebra. As in the proof of point (1), we have that $f^{-1}(U) = \mathrm{Spec}(B)$, with $B \cong \prod_{i=1}^{n} B_i$ as A-algebras. By lemma 2.1.64, we have that B is a projective separable A-algebra. Since this holds for every open affine subset $U = \mathrm{Spec}(A)$ of X, by lemma 2.2.10(4) we have that f is finite étale.
Conversely, assume that f is finite étale. Let $U = \mathrm{Spec}(A)$ be an open affine subset of X. By lemma 2.2.10(4), we have that $f^{-1}(U)$ is affine and equal to $\mathrm{Spec}(B)$, where B is a projective separable A-algebra. As in the proof of point (1), for every $i = 1, \dots, n$ there exists $s_i \in B$ such that $f_i^{-1}(U) = \mathrm{Spec}(B_{s_i})$. We have also that $B \cong \prod_{i=1}^{n} B_{s_i}$ as A-algebras. Since B is a projective separable A-algebra, by lemma 2.1.64 we have that B_{s_i} is a projective separable A-algebra for every $i = 1, \dots, n$. Since this holds for every open affine subset $U = \mathrm{Spec}(A)$ of X, by lemma 2.2.10(4) we have that f_i is finite étale for every $i = 1, \dots, n$.

□

Remark 2.2.19. We can compare lemma 2.2.18 to what happens with finite coverings of topological spaces: if $f_1 : Y_1 \to X, \dots, f_n : Y_n \to X$ are finite coverings of a topological space X, then gluing them we get a finite covering $f : \coprod_{i=1}^{n} Y_i \to X$ (see the proof of (G2) in the proposition 1.8 in the appendix) and

$$|f^{-1}(\{x\})| = \left|\coprod_{i=1}^{n} f_i^{-1}(\{x\})\right| = \sum_{i=1}^{n} |f_i^{-1}(\{x\})| ,$$

for any $x \in X$ (this equality corresponds to 2.2.18(2)).

Lemma 2.2.20. *Let $(X_i)_{i \in I}$, $(Y_i)_{i \in I}$ be two collections of schemes. Define $X := \coprod_{i \in I} X_i$ and $Y := \coprod_{i \in I} Y_i$ (disjoint union of schemes). Moreover, for every $i \in I$ let $f_i : Y_i \to X_i$ be a finite and locally free (respectively, finite étale) morphism of schemes. Let $f : Y \to X$ be the induced morphism of schemes. Then f is finite and locally free (respectively, finite étale).*

Proof. Assume that f_i is finite and locally free for every $i \in I$. Then, for every $i \in I$, there exists a cover of X_i by open affine subsets $(U_{ij} = \mathrm{Spec}(A_{ij}))_{j \in J_i}$ such that, for every $j \in J_i$, $f_i^{-1}(U_{ij})$ is affine and equal to $\mathrm{Spec}(B_{ij})$, where the A_{ij}-algebra B_{ij} is finitely generated and free as an A_{ij}-module. Since $X = \coprod_{i \in I} X_i$, we have that $(U_{ij} = \mathrm{Spec}(A_{ij}))_{i \in I, j \in J_i}$ is a cover of X by open affine subsets. Moreover, by definition of f, we have that $f^{-1}(U_{ij}) = f_i^{-1}(U_{ij}) = \mathrm{Spec}(B_{ij})$ for every $i \in I$, $j \in J_i$. So the cover $(U_{ij} = \mathrm{Spec}(A_{ij}))_{i \in I, j \in J_i}$ has the property required in the definition 2.2.3(3). Then f is finite and locally free.
Assume now that f_i is finite étale for every $i \in I$. Then, for every $i \in I$, there exists a cover of X_i by open affine subsets $(U_{ij} = \mathrm{Spec}(A_{ij}))_{j \in J_i}$ such that, for every $j \in J_i$,

$f_i^{-1}(U_{ij})$ is affine and equal to $\mathrm{Spec}(B_{ij})$, where B_{ij} is a free separable A_{ij}-algebra. As above, we have that $(U_{ij} = \mathrm{Spec}(A_{ij}))_{i \in I, j \in J_i}$ is a cover of X by open affine subsets and $f^{-1}(U_{ij}) = f_i^{-1}(U_{ij}) = \mathrm{Spec}(B_{ij})$ for every $i \in I$, $j \in J_i$. So the cover $(U_{ij} = \mathrm{Spec}(A_{ij}))_{i \in I, j \in J_i}$ has the property required in the definition 2.2.1. Then f is finite étale. □

Remark 2.2.21. A similar result holds for finite coverings of topological spaces: if $f_i : Y_i \to X_i$ is a finite covering of the topological space X_i for any $i \in I$, then gluing them we get a finite covering $f : \coprod_{i \in I} Y_i \to \coprod_{i \in I} X_i$. Indeed, let $x \in X_i$. Then there exists a unique $j \in I$ such that $x \in X_j$. Since f_j is a finite covering of X_j, there exists an open neighbourhood U of x in X_j such that $f_j : f_j^{-1}(U) \to U$ is a trivial covering. Then U is also an open neighbourhood of x in $\coprod_{i \in I} X_i$ and, by definition of f, we have that $f^{-1}(U) = f_j^{-1}(U)$ and $f_{|_{f^{-1}(U)}} = (f_j)_{|_{f_j^{-1}(U)}} : f^{-1}(U) = f_j^{-1}(U) \to U$ is a trivial covering. Finiteness follows from the fact that $f^{-1}(\{x\}) = f_j^{-1}(\{x\})$.

Lemma 2.2.22. *Let X, Y be schemes and $f : Y \to X$ a finite and locally free (respectively, finite étale) morphism. Then, for every open subscheme X' of X, the restriction $f_{|_{f^{-1}(X')}} : f^{-1}(X') \to X'$ is finite and locally free (respectively, finite étale) and $[f^{-1}(X') : X'] = [Y : X]_{|_{\mathrm{sp}(X')}}$.*

Proof. First of all, notice that $f^{-1}(X')$ is an open subscheme of Y by the continuity of f and that the restriction of f to this open subscheme is again a morphism of schemes.
Assume that f is finite and locally free and let $U = \mathrm{Spec}(A)$ be an open affine subset of X'. Then U is also an open affine subset of X and, by lemma 2.2.10(3), we have that $f^{-1}(U)$ is affine and equal to $\mathrm{Spec}(B)$, where B is a finite projective A-algebra. But, since $U \subseteq X'$, we have that $f^{-1}(U) = \left(f_{|_{f^{-1}(X')}}\right)^{-1}(U)$. Then, by lemma 2.2.10(3), we have that $f_{|_{f^{-1}(X')}}$ is finite and locally free.
Assume now that f is finite étale. For any open affine subset $U = \mathrm{Spec}(A)$ of X', by lemma 2.2.10(4) we have that $\left(f_{|_{f^{-1}(X')}}\right)^{-1}(U) = f^{-1}(U)$ is affine and equal to $\mathrm{Spec}(B)$, where B is a projective separable A-algebra. Then, by the same lemma, $f_{|_{f^{-1}(X')}}$ is finite étale.
Finally, let $U = \mathrm{Spec}(A)$ be an open affine subset of X'. Let d_U and d'_U be defined as in lemma 2.2.12, considering respectively f and $f_{|_{f^{-1}(X')}}$. As above, we have that $\left(f_{|_{f^{-1}(X')}}\right)^{-1}(U) = f^{-1}(U) = \mathrm{Spec}(B)$ for a finite projective A-algebra B. Then $d_U = [B : A] = d'_U$. Since X' is covered by its open affine subsets, it follows that $[f^{-1}(X') : X'] = [Y : X]_{|_{\mathrm{sp}(X')}}$. □

Remark 2.2.23. A similar result holds for finite coverings of topological spaces: if $f : Y \to X$ is a finite covering of the topogical space X and X' is a subset of X, then the restriction $f_{|_{f^{-1}(X')}} : f^{-1}(X') \to X'$ is a finite covering of X'. Indeed, let $x \in X'$. Since f is a finite covering of X, there exist an open neighbourhood U of x in X, a finite discrete topological space E and a homeomorphism $\varphi : f^{-1}(U) \to U \times E$ such that $p_U \circ \varphi = f$, where $p_U : U \times E \to U$ is the projection on the first factor. Define

$U' := U \cap X' \subseteq X'$. We have that $x \in U \cap X' = U'$ and U' is open in X', because U is open in X. So U' is an open neighbourhood of x in X'. Since $U' \subseteq U$ and $p_U \circ \varphi = f$, we have that

$$\left(f_{|_{f^{-1}(X')}}\right)^{-1}(U') = f^{-1}(U') = (p_U \circ \varphi)^{-1}(U') = \varphi^{-1}(p_U^{-1}(U')) = \varphi^{-1}(U' \times E) .$$

Then, restricting φ to $f^{-1}(U')$ we get a homeomorphism $\varphi : f^{-1}(U') = \varphi^{-1}(U' \times E) \to U' \times E$. The equality $p_U \circ \varphi = f$ is still true when we consider the restrictions, so $p_{U'} \circ \varphi = f_{|_{f^{-1}(X')}}$, where $p'_U : U' \times E \to U'$ is the projection on the first factor (which is clearly the restriction of p_U). This shows that $f_{|_{f^{-1}(X')}} : f^{-1}(X') \to X'$ is a finite covering of X'. Moreover, for any $x \in X'$ we have that $\left(f_{|_{f^{-1}(X')}}\right)^{-1}(\{x\}) = f^{-1}(\{x\})$ and so

$$\left|\left(f_{|_{f^{-1}(X')}}\right)^{-1}(\{x\})\right| = \left|f^{-1}(\{x\})\right| ,$$

which corresponds to the statement about the degree.
Notice that we do not need X' to be open. On the other hand, in the case of schemes we considered only open subsets because they have a natural induced scheme structure, unlike arbitrary subsets.

Corollary 2.2.24. *Let $(X_i)_{i\in I}$ be a collections of schemes and define $X := \coprod_{i\in I} X_i$ (disjoint union of schemes). Moreover, let Y be a scheme and $f : Y \to X$ a finite and locally free (respectively, finite étale) morphism of schemes. Then, if we define $Y_i := f^{-1}(X_i)$ and $f_i = f_{|_{Y_i}} : Y_i = f^{-1}(X_i) \to X_i$ for every $i \in I$, we have that $Y = \coprod_{i\in I} Y_i$ and $f_i : Y_i \to X_i$ is finite and locally free (respectively, finite étale) for any $i \in I$ (notice that this is in a certain sense the converse of lemma 2.2.20). Moreover, $[Y_i : X_i] = [Y : X]_{|_{\mathrm{sp}(X_i)}}$ for any $i \in I$.*

Proof. For any $i \in I$ we have that X_i is an open subscheme of X (by definition of disjoint union of schemes) and so $Y_i = f^{-1}(X_i)$ is an open subscheme of Y, by the continuity of f. Then we have that

$$Y = f^{-1}(X) = f^{-1}\left(\coprod_{i\in I} X_i\right) = \coprod_{i\in I} f^{-1}(X_i) = \coprod_{i\in I} Y_i$$

as schemes. The rest of the claim follows immediately from lemma 2.2.22. □

Remark 2.2.25. A similar result holds for finite coverings of topological spaces: if $f : Y \to X$ is a finite covering of the topological space X and $X = \coprod_{i\in I} X_i$ (disjoint union of topological spaces), then we can define $Y_i := f^{-1}(X_i)$ and $f_i = f_{|_{Y_i}} : Y_i = f^{-1}(X_i) \to X_i$ for every $i \in I$. Then, since f is continuous, we have that Y_i is open in Y for any $i \in I$ (recall that X_i is open in X by definition of disjoint union) and so

$$Y = f^{-1}(X) = f^{-1}\left(\coprod_{i\in I} X_i\right) = \coprod_{i\in I} f^{-1}(X_i) = \coprod_{i\in I} Y_i$$

as topological spaces. Moreover, by remark 2.2.23, for any $i \in I$ we have that $f_i : Y_i \to X_i$ is a finite covering of X_i and $|f^{-1}(\{x\})| = |f_i^{-1}(\{x\})|$ for every $x \in X_i$.

Corollary 2.2.26. *Let X, Y be schemes and $f : Y \to X$ a finite and locally free morphism. Define*

$$X_{\geq 1} = \{x \in \mathrm{sp}(X) \mid [Y : X](x) \geq 1\} \subseteq \mathrm{sp}(X) \ .$$

Then:

(1) $X_{\geq 1}$ is both open and closed in $\mathrm{sp}(X)$;

(2) $X_{\geq 1}$ is the (set-theoretic) image of f.

In particular, this holds also for any finite étale morphism f (because finite étale implies finite and locally free, see remark 2.2.4).

Proof. (1) We have that $X_{\geq 1} = [Y : X]^{-1}(\{n \in \mathbb{Z} \mid n \geq 1\})$. Then $X_{\geq 1}$ is both open and closed in $\mathrm{sp}(X)$ because $[Y : X] : \mathrm{sp}(X) \to \mathbb{Z}$ is continuous and $\{n \in \mathbb{Z} \mid n \geq 1\}$ is open in $\mathbb{Z}$ (which has the discrete topology).

(2) Since $X_{\geq 1}$ is open, by lemma 2.2.22 the restriction $f : f^{-1}(X_{\geq 1}) \to X_{\geq 1}$ is finite and locally free and $[f^{-1}(X_{\geq 1}) : X_{\geq 1}](x) = [Y : X](x) \geq 1$ for any $x \in X_{\geq 1}$. By lemma 2.2.15(3), we have that $f : f^{-1}(X_{\geq 1}) \to X_{\geq 1}$ is surjective. This means that $X_{\geq 1} = f(f^{-1}(X_{\geq 1}))$. Define now $X_0 := X \backslash X_{\geq 1}$. By definition, the degree has values that are non-negative integers. So $X_0 = \{x \in \mathrm{sp}(X) \mid [Y : X](x) = 0\}$. Since $X_{\geq 1}$ is closed, we have that X_0 is open. So, by lemma 2.2.22, the restriction $f : f^{-1}(X_0) \to X_0$ is finite and locally free and $[f^{-1}(X_0) : X_0](x) = [Y : X](x) = 0$ for any $x \in X_0$. By lemma 2.2.15(1), it follows that $f^{-1}(X_0) = \emptyset$. Then

$$\begin{aligned} Y = f^{-1}(X) = f^{-1}(X_{\geq 1} \cup X_0) = \\ = f^{-1}(X_{\geq 1}) \cup f^{-1}(X_0) = f^{-1}(X_{\geq 1}) \cup \emptyset = f^{-1}(X_{\geq 1}) \ , \end{aligned}$$

which implies that $X_{\geq 1} = f(f^{-1}(X_{\geq 1})) = f(Y)$.

□

Remark 2.2.27. A similar result holds for finite coverings of topological spaces: if $f : Y \to X$ is a finite covering of the topological space X, then

$$\mathrm{Im}(f) = \{x \in X \mid |f^{-1}(x)| \geq 1\} \ ,$$

which is both open and closed in X by the continuity of the degree (see remark 1.2(2) in the appendix).

Lemma 2.2.28. *Let X, Y and W be schemes. Let $f : Y \to X$ be a finite and locally free morphism of schemes and $g : W \to X$ any morphism of schemes. Consider the fibred product $Y \times_X W$ (see [4], chapter II, theorem 3.3), with the projections $p_1 : Y \times_X W \to Y$ and $p_2 : Y \times_X W \to W$. Then:*

(1) $p_2 : Y \times_X W \to W$ is finite and locally free;

(2) the diagram

$$\begin{array}{ccc} \mathrm{sp}(W) & \xrightarrow{\;g\;} & \mathrm{sp}(X) \\ & \searrow^{[Y \times_X W : W]} & \big\downarrow [Y : X] \\ & & \mathbb{Z} \end{array}$$

is commutative;

(3) if f is surjective, then $p_2 : Y \times_X W \to W$ is surjective;

(4) if f is finite étale, then $p_2 : Y \times_X W \to W$ is finite étale.

Proof. (1) Since f is finite and locally free, there exists a cover of X by open affine subsets $(U_i = \mathrm{Spec}(A_i))_{i \in I}$ such that, for every $i \in I$, $f^{-1}(U_i)$ is affine and equal to $\mathrm{Spec}(B_i)$, where the A_i-algebra B_i is finitely generated and free as an A_i-module. Let $i \in I$. We have that $g^{-1}(U_i)$ is an open subscheme of W (because g is a morphism of schemes). So we can cover $g^{-1}(U_i)$ with open affine subsets $(V_{ij} = \mathrm{Spec}(C_{ij}))_{j \in J_i}$. Fix $j \in J_i$ and consider $p_2^{-1}(V_{ij}) \subseteq Y \times_X W$. We claim that $p_2^{-1}(V_{ij}) = f^{-1}(U_i) \times_{U_i} V_{ij}$. By definition of fibred product, we have $f \circ p_1 = g \circ p_2$. Then $p_1^{-1}(f^{-1}(U_i)) = p_2^{-1}(g^{-1}(U_i))$. Since $V_{ij} \subseteq g^{-1}(U_i)$, we get that $p_2^{-1}(V_{ij}) \subseteq p_2^{-1}(g^{-1}(U_i)) = p_1^{-1}(f^{-1}(U_i))$. Consider the following diagram.

$$\begin{array}{ccc} p_2^{-1}(V_{ij}) & \xrightarrow[p_2]{} & V_{ij} \\ \big\downarrow p_1 & & \big\downarrow g \\ f^{-1}(U_i) & \xrightarrow{\;f\;} & U_i \end{array}$$

The equality $f \circ p_1 = g \circ p_2$ is still satisfied when we consider the restrictions $p_1 : p_2^{-1}(V_{ij}) \subseteq p_1^{-1}(f^{-1}(U_i)) \to f^{-1}(U_i)$, $p_2 : p_2^{-1}(V_{ij}) \to V_{ij}$, $f : f^{-1}(U_i) \to U_i$ and $g : V_{ij} \subseteq g^{-1}(U_i) \to U_i$. Let now Z be a scheme with two morphisms of schemes $h_1 : Z \to f^{-1}(U_i)$, $h_2 : Z \to V_{ij}$ such that $f \circ h_1 = g \circ h_2$. Since $f^{-1}(U_i) \subseteq Y$, we can see h_1 as a morphism of schemes $Z \to Y$. Analogously, since $V_{ij} \subseteq W$, we can see p_2 as a morphism of schemes $Z \to W$. Then, by the universal property of the fibred product, there exists a unique $h : Z \to Y \times_X W$ such that $h_1 = p_1 \circ h$ and $h_2 = p_2 \circ h$. Then $p_2(h(Z)) = h_2(Z) \subseteq V_{ij}$ and so $h(Z) \subseteq p_2^{-1}(V_{ij})$. Then we can see h as a morphism of schemes $Z \to p_2^{-1}(V_{ij})$ such that $h_1 = p_1 \circ h$ and $h_2 = p_2 \circ h$. Moreover, it is the unique such morphism, because we know uniqueness when considering h as a morphism $Z \to Y \times_X W$. This proves that $p_2^{-1}(V_{ij}) = f^{-1}(U_i) \times_{U_i} V_{ij}$. Recall that $U_i = \mathrm{Spec}(A_i)$, $f^{-1}(U_i) = \mathrm{Spec}(B_i)$ and $V_{ij} = \mathrm{Spec}(C_{ij})$. Then

$$p_2^{-1}(V_{ij}) = f^{-1}(U_i) \times_{U_i} V_{ij} = \mathrm{Spec}(B_i) \times_{\mathrm{Spec}(A_i)} \mathrm{Spec}(C_{ij}) = \mathrm{Spec}(B_i \otimes_{A_i} C_{ij})$$

(see the proof of theorem 3.3 in chapter II of [4]). Since B_i is finitely generated and free as an A_i-module, we have that $B_i \cong A_i^{n_i}$ for some $n_i \in \mathbb{N}$. Since tensor product and direct sums commute (lemma 2.1.19), it follows that

$$B_i \otimes_{A_i} C_{ij} \cong A_i^{n_i} \otimes C_{ij} \cong (A_i \otimes C_{ij})^{n_i} \cong C_{ij}^{n_i}$$

as C_{ij}-modules (lemma 2.1.19 gives an isomorphism of A_i-modules, but it is immediate to check that in this case that isomorphism is also C_{ij}-linear). So $B_i \otimes_{A_i} C_{ij}$ is finitely generated and free as a C_{ij}-module. This holds for any $i \in I$, $j \in J_i$. Now we have that

$$W = p_2^{-1}(X) = p_2^{-1}\left(\bigcup_{i\in I} U_i\right) = \bigcup_{i\in I} p_2^{-1}(U_i) = \bigcup_{i\in I}\bigcup_{j\in J_i} V_{ij} \,.$$

So $(V_{ij} = \mathrm{Spec}(C_{ij}))_{i\in I, j\in J_i}$ is a cover of W by open affine subsets. This cover has the property required in the definition 2.2.3(3), so p_2 is finite and locally free.

(2) Let $(U_i = \mathrm{Spec}(A_i))_{i\in I}$, $(V_{ij} = \mathrm{Spec}(C_{ij}))_{i\in I, j\in J_i}$ be as in the proof of point (1). For every $i \in I$, let d_{U_i} be defined as in lemma 2.2.12. Analogously, for any $i \in I$, $j \in J_i$, let $d_{V_{ij}}$ be defined as in lemma 2.2.12 (considering the morphism p_2). Fix $i \in I$, $j \in J_i$ and define $n_i := \mathrm{rank}_{A_i}(B_i)$. This means that $B_i \cong A_i^{n_i}$ as an A_i-module. As in the proof of point (1), this implies that $B_i \otimes_{A_i} C_{ij} \cong C_{ij}^{n_i}$ as C_{ij}-modules. Then $\mathrm{rank}_{C_{ij}}(B_i \otimes_{A_i} C_{ij}) = n_i = \mathrm{rank}_{A_i}(B_i)$. Recalling that $p_2^{-1}(V_{ij}) = \mathrm{Spec}(B_i \otimes_{A_i} C_{ij})$ and using remark 2.1.36(1), we get that

$$\begin{aligned}[Y \times_X W : W](w) = d_{V_{ij}}(w) = [B_i \otimes_{A_i} C_{ij} : C_{ij}](x) = \mathrm{rank}_{C_{ij}}(B_i \otimes_{A_i} C_{ij}) = \\ = \mathrm{rank}_{A_i}(B_i) = [B_i : A_i](g(w)) = d_{U_i}(g(w)) = [Y : X](g(w))\end{aligned}$$

for every $w \in V_{ij}$ (in this case $g(w) \in U_i$, because $V_{ij} \subseteq g^{-1}(U_i)$). Since this holds for any $i \in I$, $j \in J_i$ and since $W = \bigcup_{i\in I}\bigcup_{j\in J_i} V_{ij}$, it follows that $[Y \times_X W : W] = [Y : X] \circ g$, as we wanted.

(3) Since f is surjective, by lemma 2.2.15(3) we have that $[Y : X] \geq 1$. Then, by point (2), we have that $[Y \times_X W : W](w) = [Y : X](g(w)) \geq 1$ for every $w \in W$. So $[Y \times_X W : W] \geq 1$, which implies that p_2 is surjective, by lemma 2.2.15(3).

(4) Since f is finite étale, there exists a cover of X by open affine subschemes $(U_i = \mathrm{Spec}(A_i))_{i\in I}$ such that, for every $i \in I$, $f^{-1}(U_i)$ is affine and equal to $\mathrm{Spec}(B_i)$, where the B_i is a free separable A_i-algebra. As in the proof of point (1), for every $i \in I$ we can cover $g^{-1}(U_i)$ with open affine subsets $(V_{ij} = \mathrm{Spec}(C_{ij}))_{j\in J_i}$ and for every $j \in J_i$ we have that $p_2^{-1}(V_{ij}) = \mathrm{Spec}(B_i \otimes_{A_i} C_{ij})$. As in the proof of point (1), we have that $(V_{ij} = \mathrm{Spec}(C_{ij}))_{i\in I, j\in J_i}$ is a cover of W by open affine subsets. Fix now $i \in I$, $j \in J_i$. Since B_i is a free separable A_i-algebra, it is in particular finitely generated and free as an A_i-module. As in the proof of point (1), this implies that $B_i \otimes_{A_i} C_{ij}$ is finitely generated and free as a C_{ij}-module. On the other hand, since B_i is a free separable A_i-algebra, it is in particular projective separable (see remark 2.1.61). Then, by lemma 2.1.71, we have that $B_i \otimes_{A_i} C_{ij}$ is a projective separable C_{ij}-algebra. Applying again remark 2.1.61, we get that $B_i \otimes_{A_i} C_{ij}$ is a free separable C_{ij}-algebra. So the

cover $(V_{ij} = \mathrm{Spec}(C_{ij}))_{i \in I, j \in J_i}$ has the property required in the definition 2.2.1. Hence p_2 is finite étale.

□

Remark 2.2.29. We can compare lemma 2.2.28 to what happens with finite coverings of topological spaces: if $f : Y \to X$ is a finite covering of X and $g : W \to X$ is any continuous function, then the projection on the second factor $p_2 : Y \times_X W \to W$ is a finite covering of W (see remark 1.12(2) in the appendix, noticing that in that part of the argument we did not use the base points and that the order of the factors in the fibered product is not important). Moreover, for any $w \in W$ we have that

$$\begin{aligned} p_2^{-1}(\{w\}) = \{(y, w') \in Y \times_X W \mid w' = p_2((y, w')) = w\} = \\ = \{(y, w) \mid y \in Y, f(y) = g(w)\} = \{(y, w) \mid y \in f^{-1}(\{g(w)\})\} \end{aligned}$$

and so $|p_2^{-1}(\{w\})| = |f^{-1}(\{g(w)\})|$, which corresponds to 2.2.28(2). This implies also that, if f is surjective, then $|p_2^{-1}(\{w\})| = |f^{-1}(\{g(w)\})| \geq 1$ for any $w \in W$ and so p_2 is surjective. Notice that this last statement (if f is surjective, then p_2 is surjective) is true for any fibred product of topological spaces: you do not need the fact that f is a finite covering. On the other hand, in the proof of lemma 2.2.28(3) we used the fact that f was finite and locally free. It is actually true that surjectivity of morphisms of schemes is preserved by base changes (see [5], exercise 9.4.D), but the proof in the general case is more complicated. It cannot be reduced to the topological result, because the underlying topological space of a fibred product of schemes is not the fibred product of the underlying topological spaces (see [4], chapter II, exercise 3.9).

Lemma 2.2.30. *The composition of finite and locally free (respectively, finite étale) morphisms is finite and locally free (respectively, finite étale).*

Proof. Let X, Y and Z be schemes and let $f : Y \to X$, $g : Z \to Y$ be two finite and locally free morphisms. Let $U = \mathrm{Spec}(A)$ be an open affine subset of X. Since f is finite and locally free, by lemma 2.2.10(3) we have that $f^{-1}(U)$ is affine and equal to $\mathrm{Spec}(B)$, where B is a finite projective A-algebra. Then, since g is finite and locally free, by lemma 2.2.10(3) we have that $(f \circ g)^{-1}(U) = g^{-1}(f^{-1}(U)) = g^{-1}(\mathrm{Spec}(B))$ is affine and equal to $\mathrm{Spec}(C)$, where C is a finite projective B-algebra. Notice that the A-algebra structure induced on C by the morphism of schemes $f \circ g : \mathrm{Spec}(C) \to \mathrm{Spec}(A)$ coincides with the one induced by the B-algebra structure. So C is a finite projective A-algebra, by corollary 2.1.54. Since this holds for every open affine subset $U = \mathrm{Spec}(A)$ of X, by lemma 2.2.10(3) we have that $f \circ g$ is finite and locally free. Assume now that f and g are finite étale and $U = \mathrm{Spec}(A)$ be an open affine subset of X. Since f is finite étale, by lemma 2.2.10(4) we have that $f^{-1}(U)$ is affine and equal to $\mathrm{Spec}(B)$, where B is a projective separable A-algebra. Then, since g is finite étale, by lemma 2.2.10(4) we have that $(f \circ g)^{-1}(U) = g^{-1}(f^{-1}(U)) = g^{-1}(\mathrm{Spec}(B))$ is affine and equal to $\mathrm{Spec}(C)$, where C is a projective separable B-algebra. As above, the A-algebra structure induced on C by the morphism of schemes $f \circ g : \mathrm{Spec}(C) \to \mathrm{Spec}(A)$ coincides with the one induced by the B-algebra structure. So C is a projective separable A-algebra, by corollary 2.1.69. Since this holds for every open affine subset $U = \mathrm{Spec}(A)$ of X, by lemma 2.2.10(4) we have that $f \circ g$ is finite étale. $\square$

Remark 2.2.31. A similar result holds for finite coverings of topological spaces: if X, Y and Z are topological spaces, $f : Y \to X$ is a finite covering of X and $g : Z \to Y$ is a finite covering of Y, then $f \circ g : Z \to X$ is a finite covering of X. Indeed, let $x \in X$. Since f is a finite covering of X, there exist an open neighbourhood U of x in X, a finite discrete topological space E and a homeomorphism $\varphi : f^{-1}(U) \to U \times E$ such that $p_U \circ \varphi = f$, where $p_U : U \times E \to U$ is the projection on the first factor. Since E has the discrete topology, we have that $U \times \{e\}$ is open in $U \times E$ for any $e \in E$ and so $U \times E = \coprod_{e \in E} U \times \{e\}$ (topological disjoint union). Then we have that

$$f^{-1}(U) = \varphi^{-1}\left(\coprod_{e \in E} U \times \{e\}\right) = \coprod_{e \in E} \varphi^{-1}(U \times \{e\})$$

(disjoint union of topological spaces). For any $e \in E$, define $V_e := \varphi^{-1}(U \times \{e\})$, so that $f^{-1}(U) = \coprod_{e \in E} V_e$. Since g is a finite covering of Y, we have that its restriction $g : g^{-1}(f^{-1}(U)) \to f^{-1}(U)$ is a finite covering of $f^{-1}(U)$ (remark 2.2.23). By remark 2.2.25, we have that $g_{|_{g^{-1}(V_e)}} : g^{-1}(V_e) \to V_e$ is a finite covering of V_e, for any $e \in E$. Since $f^{-1}(U) = \coprod_{e \in E} V_e$, we have that

$$(f \circ g)^{-1}(U) = g^{-1}(f^{-1}(U)) = g^{-1}\left(\coprod_{e \in E} V_e\right) = \coprod_{e \in E} g^{-1}(V_e) \ .$$

Let now $e \in E$. We claim that $f \circ g : g^{-1}(V_e) \to U$ is a finite covering. Define $q_e : U \to U \times \{e\}$, $x' \mapsto (x', e)$, which is continuous because its components (respectively, the identity and a constant function) are continuous. We have that q_e is bijective, with inverse the restricted projection $p_U : U \times \{e\} \to U$, which is also continuous by definition of product topology. So q_e is a homeomorphism. It follows that $\varphi^{-1} \circ q_e : U \to \varphi^{-1}(U \times \{e\}) = V_e$ is also a homeomorphism, because it is a composition of homeomorphisms. Let $x' \in U$ and consider $y := (\varphi^{-1} \circ q_e)(x') \in V_e$. Since $g : g^{-1}(V_e) \to V_e$ is a finite covering, there exist an open neighbourhood W of y in V_e, a finite discrete topological space F and a homeomorphism $\psi : g^{-1}(W) \to W \times F$ such that $p_W \circ \psi = g$, where $p_W : W \times F \to W$ is the projection on the first factor. Define $U' := (p_U \circ \varphi)(W) = (\varphi^{-1} \circ q_e)^{-1}(W)$. Since $\varphi^{-1} \circ q_e : U \to V_e$ is continuous and W is open in V_e, we have that U' is open in U. Moreover, since $y = (\varphi^{-1} \circ q_e)(x') \in W$, we have that $x' \in (\varphi^{-1} \circ q_e)^{-1}(W) = U'$. Notice that, since $U' \subseteq U$ and $p_U \circ \varphi = f$,

$$f^{-1}(U') \cap V_e = (p_U \circ \varphi)^{-1}((p_U \circ \varphi)(W)) \cap V_e = W$$

(the last equality follows from the fact that $W \subseteq V_e$ and that $p_U \circ \varphi : V_e \to U$ is bijective). So $(f \circ g)^{-1}(U') \cap g^{-1}(V_e) = g^{-1}(f^{-1}(U')) \cap g^{-1}(V_e) = g^{-1}(f^{-1}(U') \cap V_e) = g^{-1}(W)$. Since $\varphi^{-1} \circ q_e$ is a homeomorphism, we have that also its restriction $\varphi^{-1} \circ q_e : (\varphi^{-1} \circ q_e)^{-1}(W) = U' \to W$ is a homeomorphism. Its inverse $p_U \circ \varphi : W \to U'$ induces a homeomorphism $(p_U \circ \varphi) \times \mathrm{id}_F : W \times F \to U' \times F$. Composing it with ψ, we get a homeomorphism

$$((p_U \circ \varphi) \times \mathrm{id}_F) \circ \psi : g^{-1}(W) = (f \circ g)^{-1}(U') \cap g^{-1}(V_e) \to U' \times F \ .$$

Denote by $p_{U'} : U' \times F \to F$ the projection on the first factor. Notice that

$$(p'_U \circ ((p_U \circ \varphi) \times \mathrm{id}_F))(w, f) = p'_U((p_U \circ \varphi)(w), f) = (p_U \circ \varphi)(w) = (p_U \circ \varphi)(p_W((w, f)))$$

for any $w \in W$, $f \in F$, and so $p'_U \circ ((p_U \circ \varphi) \times \mathrm{id}_F) = p_U \circ \varphi \circ p_W$. Then, recalling that $p_W \circ \psi = g$ and $p_U \circ \varphi = f$, we have that

$$p_{U'} \circ (((p_U \circ \varphi) \times \mathrm{id}_F) \circ \psi) = p_U \circ \varphi \circ p_W \circ \psi = f \circ g \ .$$

So $f \circ g : (f \circ g)^{-1}(U') \cap g^{-1}(V_e) \to U'$ is a finite trivial covering (finiteness follows from the fact that F is finite). This shows that $f \circ g : g^{-1}(V_e) \to U$ is a finite covering of U, for any $e \in E$. By remark 2.2.19, we have that $f \circ g : \coprod_{e \in E} g^{-1}(V_e) = (f \circ g)^{-1}(U) \to U$ is a finite covering of U (recall that E is finite). Then there exists an open neighbourhood U'' of x in U such that $f \circ g : (f \circ g)^{-1}(U'') \to U''$ is a finite trivial covering. Since U is open in X, we have that U'' is open also in X. So U'' is an open neighbourhood of x in X and $f \circ g : (f \circ g)^{-1}(U'') \to U''$ is a finite trivial covering. This shows that $f \circ g$ is a finite covering of X.

Lemma 2.2.32. *Let X, Y and Z be schemes, $f : Y \to X$ and $g : Z \to X$ finite and locally free morphisms of schemes. Consider the fibred product $Y \times_X Z$, with the projections $p_1 : Y \times_X Z \to Y$ and $p_2 : Y \times_X Z \to Z$. Then:*

(1) $f \circ p_1 = g \circ p_2 : Y \times_X Z \to X$ is finite and locally free;

(2) if f and g are surjective, then $f \circ p_1 = g \circ p_2 : Y \times_X Z \to X$ is surjective;

(3) if f and g are finite étale, then $f \circ p_1 = g \circ p_2 : Y \times_X Z \to X$ is finite étale.

Proof. Recall that $f \circ p_1 = g \circ p_2$ by definition of fibred product.

(1) Since f is finite and locally free, by lemma 2.2.28(1) we have that $p_2 : Y \times_X Z \to Z$ is finite and locally free. Then, since g is finite and locally free, by lemma 2.2.30 we have that the composition $g \circ p_2$ is also finite and locally free.

(2) Since f is surjective, by lemma 2.2.28(3) we have that $p_2 : Y \times_X Z \to Z$ is surjective. Then, since g is surjective, the composition $g \circ p_2$ is also surjective.

(3) Since f is finite étale, by lemma 2.2.28(4) we have that $p_2 : Y \times_X Z \to Z$ is finite étale. Then, since g is finite étale, by lemma 2.2.30 we have that the composition $g \circ p_2$ is also finite étale.

□

Remark 2.2.33. Combining the remarks 2.2.29 and 2.2.31, we get that a similar result is true for finite coverings of topological spaces: if $f : Y \to X$ and $g : Z \to X$ are finite coverings of a topological space X, then $f \circ p_1 = g \circ p_2 : Y \times_X Z \to X$ is also a finite covering of X, where $p_1 : Y \times_X Z \to Y$ and $p_2 : Y \times_X Z \to Z$ are the two projections.

Now we know that finite étale morphisms are preserved by base changes (lemma 2.2.28(4)). If we restrict our attention to base extensions that are surjective, finite and locally free, we have also a "converse" result.

Lemma 2.2.34. *Let X, Y and W be schemes, $f : Y \to X$ and $g : W \to X$ morphisms of schemes, with f affine and g surjective, finite and locally free. Consider the fibred product $Y \times_X W$ with the projections $p_1 : Y \times_X W \to Y$ and $p_2 : Y \times_X W \to W$. Then f is finite étale (respectively, finite and locally free) if and only if p_2 is finite étale (respectively, finite and locally free).*

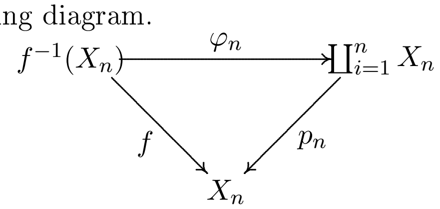
Proof. By lemma 2.2.28(4) (respectively, (3)), if f is finite étale (respectively, finite and locally free) then p_2 is also finite étale (respectively, finite and locally free).
Conversely, assume that p_2 is finite étale (respectively, finite and locally free) and let $U = \mathrm{Spec}(A)$ be an open affine subset of X. Since f is affine, by lemma 2.2.10(1) we have that $f^{-1}(U)$ is affine. Then $f^{-1}(U) = \mathrm{Spec}(B)$ for an A-algebra B. Since g is surjective, finite and locally free, by corollary 2.2.17 we have that $g^{-1}(U)$ is affine and equal to $\mathrm{Spec}(C)$, where C is a faithfully projective A-algebra. By definition of fibred product, we have that $f \circ p_1 = g \circ p_2$. Then $p_1^{-1}(f^{-1}(U)) = (f \circ p_1)^{-1}(U) = (g \circ p_2)^{-1}(U) = p_2^{-1}(g^{-1}(U))$. Notice that the equality $f \circ p_1 = g \circ p_2$ holds also if we consider the restrictions $p_1 : p_1^{-1}(f^{-1}(U)) = p_2^{-1}(g^{-1}(U)) \to f^{-1}(U)$, $p_2 : p_1^{-1}(f^{-1}(U)) = p_2^{-1}(g^{-1}(U)) \to g^{-1}(U)$, $f : f^{-1}(U) \to U$ and $g : g^{-1}(U) \to U$. Moreover, let Z be a scheme with two morphisms of schemes $h_1 : Z \to f^{-1}(U)$ and $h_2 : Z \to g^{-1}(U)$ such that $f \circ h_1 = g \circ h_2$. Since $f^{-1}(U) \subseteq Y$ and $g^{-1}(U) \subseteq W$, we can see h_1 as a morphism of schemes $Z \to Y$ and h_2 as a morphism of schemes $Z \to W$. Then, by the universal property of the fibred product, there exists a unique $h : Z \to Y \times_X W$ such that $h_1 = p_1 \circ h$ and $h_2 = p_2 \circ h$. Then $p_1(h(Z)) = h_1(Z) \subseteq f^{-1}(U)$ and we can see h as a morphism of schemes $Z \to p_1^{-1}(f^{-1}(U)) = p_2^{-1}(g^{-1}(U))$ such that $h_1 = p_1 \circ h$ and $h_2 = p_2 \circ h$. Moreover, it is the unique such morphism, because we know uniqueness when considering h as a morphism $Z \to Y \times_X W$. This proves that $p_2^{-1}(g^{-1}(U)) = f^{-1}(U) \times_U g^{-1}(U)$. Then

$$p_2^{-1}(g^{-1}(U)) = f^{-1}(U) \times_U g^{-1}(U) = \mathrm{Spec}(B) \times_{\mathrm{Spec}(A)} \mathrm{Spec}(C) = \mathrm{Spec}(B \otimes_A C)$$

(see the proof of theorem 3.3 in chapter II of [4]). Notice that the C-algebra structure induced on $B \otimes_A C$ by the morphism $p_2 : p_2^{-1}(g^{-1}(U)) = \mathrm{Spec}(B \otimes_A C) \to g^{-1}(U) = \mathrm{Spec}(C)$ coincides with the one that is usually induced on the tensor product. Since p_2 is finite étale (respectively, finite and locally free), by lemma 2.2.10(4) (respectively, (3)) we have that $B \otimes_A C$ is a projective separable (respectively, finite projective) C-algebra. Since C is a faithfully projective A-algebra, by 2.1.42 ((iv) $\Longrightarrow$ (i)) it is also faithfully flat. Then, by proposition 2.1.72 (respectively, 2.1.57) we have that B is a projective separable (respectively, finite projective) A-algebra. Since this holds for any open affine subset $U = \mathrm{Spec}(A)$ of X, by lemma 2.2.10(4) (respectively, (3)) we have that f is finite étale (respectively, finite and locally free). □

We will now furtherly simplify the study of finite étale morphisms by introducing another class of morphisms: totally split morphisms.

Definition 2.2.35. Let X, Y be schemes and $f : Y \to X$ a morphism of schemes. We say that f is *totally split* if we can write $X = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n$ for some schemes $X_0, X_1, \ldots$ such that, for any $n \in \mathbb{Z}$, $n \geq 0$, there exists an isomorphism of schemes $\varphi_n : f^{-1}(X_n) \to \coprod_{i=1}^{n} X_n$ such that $p_n \circ \varphi_n = f$, where $p_n : \coprod_{i=1}^{n} X_n \to X_n$ is obtained by gluing the identity morphisms $\mathrm{id}_{X_n} : X_n \to X_n$. This definition is illustrated by the following diagram.



Example 2.2.36. Any isomorphism of schemes is totally split. Indeed, if X, Y are schemes and $f : Y \to X$ is an isomorphism, we can define $X_1 := X$ and $X_n := \emptyset$ for any $n \in \mathbb{Z}$, $n \geq 0$, $n \neq 1$. Then $X = X_1 = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n$. Moreover, we can define $\varphi_1 := f : f^{-1}(X_1) = f^{-1}(X) = Y \to X$. Then we have $p_1 \circ \varphi_1 = \mathrm{id}_X \circ f = f$. This shows that f is totally split. In particular, id_X is totally split for any scheme X.

Lemma 2.2.37. *Any totally split morphism of schemes is finite étale.*

Proof. Let X, Y be schemes and $f : Y \to X$ a totally split morphism of schemes. Moreover, let $X_0, X_1, \ldots$ be as in the definition 2.2.35. Since $X = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n$, we have that $Y = f^{-1}(X) = f^{-1}\left(\coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n\right) = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} f^{-1}(X_n)$ and f can be obtained by gluing the restrictions $f_{|_{f^{-1}(X_n)}} : f^{-1}(X_n) \to X_n$. By lemma 2.2.20, in order to prove that f is finite étale, it is enough to prove that $f_{|_{f^{-1}(X_n)}} : f^{-1}(X_n) \to X_n$ is finite étale for any $n \in \mathbb{Z}$, $n \geq 0$. Fix $n \in \mathbb{Z}$, $n \geq 0$ and let $U = \mathrm{Spec}(A)$ be an open affine subset of X_n. Since $f_{|_{f^{-1}(X_n)}} = p_n \circ \varphi_n$ (where p_n and φ_n are as in the definition 2.2.35), we have that $f^{-1}(U) = (p_n \circ \varphi_n)^{-1}(U) = \varphi_n^{-1}(p_n^{-1}(U)) = \varphi_n^{-1}\left(\coprod_{i=1}^{n} U\right)$. So φ_n restricts to an isomorphism of schemes $f^{-1}(U) = \varphi_n^{-1}\left(\coprod_{i=1}^{n} U\right) \to \coprod_{i=1}^{n} U$. Then

$$f^{-1}(U) \cong \coprod_{i=1}^{n} U = \coprod_{i=1}^{n} \mathrm{Spec}(A) = \mathrm{Spec}(A^n)$$

(the last equality can be proved as in the proof of lemma 2.2.18). By example 2.1.6, we have that A^n is a free separable A-algebra. Then, by remark 2.1.61(3), A^n is a projective separable A-algebra. By lemma 2.2.10(4), $f_{|_{f^{-1}(X_n)}}$ is finite étale, as we wanted. □

Remark 2.2.38. (1) Let X, Y be schemes and $f : Y \to X$ a totally split morphism. By the lemma we have just proved, f is finite étale, so it is in particular finite and locally free and this allows us to consider its degree $[Y : X] : \mathrm{sp}(X) \to \mathbb{Z}$ (definition 2.2.14). Fix $n \in \mathbb{Z}$, $n \geq 0$ and let $U = \mathrm{Spec}(A)$ be an open affine subset of X. Let d_U be defined as in lemma 2.2.12. As in the proof of lemma 2.2.37, we have that $f^{-1}(U) = \mathrm{Spec}(A^n)$. Then $d_U = [A^n : A]$ is constantly equal to n. Since X_n is covered by open affine subsets, it follows that $[Y : X](x) = n$ for any $x \in X_n$.

(2) Totally split morphisms of constant degree are the analogue of trivial finite coverings of topological spaces. Indeed, by point (1) a totally split morphism $f : Y \to X$ has constant degree if and only if there exists at most one $n \in \mathbb{Z}$, $n \geq 0$ such that $X_n \neq \emptyset$ (if $X \neq \emptyset$, then there exists a unique such n, more precisely $n = [Y : X]$), where $X_0, X_1, \dots$ are as in the definition 2.2.35. In this case, $X = X_n$ and, as in the definition 2.2.35, we have an isomorphism of schemes $\varphi = \varphi_n : f^{-1}(X_n) = f^{-1}(X) = Y \to \coprod_{i=1}^n X_n = \coprod_{i=1}^n X$ such that $f = p \circ \varphi$, where $p = p_n : \coprod_{i=1}^n X_n = \coprod_{i=1}^n X \to X_n = X$ is obtained by gluing the identity morphisms.
On the other hand, if X, Y are topological spaces and $f : Y \to X$ is trivial finite covering of degree n, then there exist a discrete topological space E with $|E| = n$ and a homeomorphism $\varphi : Y \to X \times E$ such that $f = p_X \circ \varphi$, where $p_X : X \times E \to X$ is the projection on the first factor. Since E is discrete, we have that $E = \coprod_{e \in E}\{e\}$ and then

$$X \times E = X \times \left(\coprod_{e \in E} \{e\} \right) = \coprod_{e \in E} (X \times \{e\}) \,.$$

On the other hand, for any $e \in E$, restricting p_X we get a homeomorphism $p_E : X \times \{e\} \to X$ (with inverse $X \to X \times \{e\},\ x \mapsto (x, e)$). Gluing these homeomorphisms, we get a homeomorphism

$$\psi : X \times E = \coprod_{e \in E} (X \times \{e\}) \to \coprod_{e \in E} X \,.$$

If we define $p : \coprod_{e \in E} X \to X,\ x \mapsto x$, we have that $(p \circ \psi)((x, e)) = p(p_E((x, e))) = p_E(x, e)$ for any $x \in X$, $e \in E$ and so $p \circ \psi = p_E$. Then $\varphi' := \psi \circ \varphi : Y \to \coprod_{e \in E} X$ is a homeomorphism and $p \circ \varphi' = p \circ \psi \circ \varphi = p_E \circ \varphi = f$.

(3) Let X be a connected scheme (in particular, $X \neq \emptyset$). If $f : Y \to X$ is a totally split morphism and $X_0, X_1, \dots$ are as in the definition 2.2.35, then from $X = \coprod_{\substack{n \in \mathbb{Z} \\ n \geq 0}} X_n$ it follows that $X_n = \emptyset$ for all but one $n \in \mathbb{Z}$, $n \geq 0$. By point (2), this means that f has constant degree.

We list now some properties of totally split morphisms that are similar to those of finite étale morphisms.

Lemma 2.2.39. *Let X, $Y_1, \dots, Y_k$ be schemes ($k \in \mathbb{N}$) with totally split morphisms $f_i : Y_i \to X$ for every $i = 1, \dots, k$. Define $Y := \coprod_{i=1}^k Y_i$ (disjoint union of schemes) and consider the morphism $f : Y \to X$ obtained by gluing the f_i's. Then f is totally split.*

Proof. For any $i = 1, \dots, k$, since f_i is totally split, we can write $X = \coprod_{\substack{n \in \mathbb{Z} \\ n \geq 0}} X_{in}$ for some schemes $X_{i0}, X_{i1}, \dots$ such that, for any $n \in \mathbb{Z}$, $n \geq 0$, there exists an isomorphism of schemes $\varphi_{in} : f_i^{-1}(X_{in}) \to \coprod_{\alpha=1}^n X_{in}$ such that $p_{in} \circ \varphi_{in} = f_i$, where $p_{in} : \coprod_{\alpha=1}^n X_{in} \to X_{in}$ is obtained by gluing the identity morphisms $\mathrm{id}_{X_{in}} : X_{in} \to$

X_{in}. Let $n_1, \dots, n_k \in \mathbb{Z}$, $n_1, \dots, n_k \geq 0$ and define $X_{n_1 \dots n_k} := \bigcap_{i=1}^k X_{in_i}$. By definition of disjoint union of schemes, we have that X_{in_i} is open in X for every $i = 1, \dots, k$. Then $X_{n_1 \dots n_k}$ is open in X, because it is a finite intersection of open subsets. By definition of f, we have that $f^{-1}(X_{n_1 \dots n_k}) = \coprod_{i=1,\dots,k} f_i^{-1}(X_{n_1 \dots n_k})$. Fix $i \in \{1, \dots, k\}$. We have that $X_{n_1 \dots n_k} \subseteq X_{in_i}$ and so $f_i^{-1}(X_{n_1 \dots n_k}) \subseteq f_i^{-1}(X_{in_i})$. Since $p_{in_i} \circ \varphi_{in_i} = f_i$, we have that $f_i^{-1}(X_{n_1 \dots n_k}) = (p_{in_i} \circ \varphi_{in_i})^{-1}(X_{n_1 \dots n_k}) = \varphi_{in_i}^{-1}(p_{in_i}^{-1}(X_{n_1 \dots n_k})) = \varphi_{in_i}^{-1}(\coprod_{\alpha=1}^{n_i} X_{n_1 \dots n_k})$. Then we can restrict φ_{in_i} to an isomorphism of schemes $\varphi_{in_i} : f_i^{-1}(X_{n_1 \dots n_k}) = \varphi_{in_i}^{-1}(\coprod_{\alpha=1}^{n_i} X_{n_1 \dots n_k}) \to \coprod_{\alpha=1}^{n_i} X_{n_1 \dots n_k}$. Gluing these isomorphisms, we get an isomorphism

$$\varphi_{n_1 \dots n_k} : \coprod_{i=1}^k f_i^{-1}(X_{n_1 \dots n_k}) = f^{-1}(X_{n_1 \dots n_k}) \to \coprod_{i=1}^k \coprod_{\alpha=1}^{n_i} X_{n_1 \dots n_k} = \coprod_{\alpha=1}^{n_1+\dots+n_k} X_{n_1 \dots n_k} .$$

Let $p_{n_1 \dots n_k} : \coprod_{\alpha=1}^{n_1+\dots+n_k} X_{n_1 \dots n_k} \to X_{n_1 \dots n_k}$ be the morphism obtained by gluing the identity morphisms $\mathrm{id}_{X_{n_1 \dots n_k}} : X_{n_1 \dots n_k} \to X_{n_1 \dots n_k}$. Then, for any $i = 1, \dots, k$, we have that $(p_{n_1 \dots n_k})_{|\coprod_{\alpha=1}^{n_i} X_{n_1 \dots n_k}}$ is induced by the identity morphisms $\mathrm{id}_{X_{n_1 \dots n_k}} = (\mathrm{id}_{X_{in_i}})_{|X_{n_1 \dots n_k}}$ and so it coincides with the restriction of p_{in_i}. It follows that

$$\begin{aligned}(p_{n_1 \dots n_k} \circ \varphi_{n_1 \dots n_k})_{|f_i^{-1}(X_{n_1 \dots n_k})} = (p_{n_1 \dots n_k})_{|\coprod_{\alpha=1}^{n_i} X_{n_1 \dots n_k}} \circ (\varphi_{n_1 \dots n_k})_{|f_i^{-1}(X_{n_1 \dots n_k})} = \\ = p_{in_i} \circ \varphi_{in_i} = f_i = f_{|f_i^{-1}(X_{n_i \dots n_k})}\end{aligned}$$

for any $i = 1, \dots, k$. Then $p_{n_1 \dots n_k} \circ \varphi_{n_1 \dots n_k} = f$. Notice that, if we consider $n_1, \dots, n_k, m_1, \dots, m_k \in \mathbb{Z}$, $n_1, \dots, n_k, m_1, \dots, m_k \geq 0$ and $i \in \{1, \dots, k\}$ is such that $n_i \neq m_i$, then $X_{n_1 \dots n_k} \cap X_{m_1 \dots m_k} = \emptyset$, because $X_{n_1 \dots n_k} \subseteq X_{in_i}$, $X_{m_1 \dots m_k} \subseteq X_{im_i}$ and $X_{in_i} \cap X_{im_i} = \emptyset$. Moreover, let $x \in X$. For any $i = 1, \dots, k$, we have that $X = \coprod_{\substack{n \in \mathbb{Z} \\ n \geq 0}} X_{in}$, so there exists $n_i \in \mathbb{Z}$, $n_i \geq 0$ such that $x \in X_{in_i}$. Then $x \in \bigcap_{i=1}^k X_{in_i} = X_{n_1 \dots n_k}$. This shows that $X = \coprod_{\substack{n_1,\dots,n_k \in \mathbb{Z} \\ n_1,\dots,n_k \geq 0}} X_{n_1 \dots n_k}$. Fix now $n \in \mathbb{Z}$, $n \geq 0$ and define $X_n := \coprod_{\substack{n_1,\dots,n_k \in \mathbb{Z},\, n_1,\dots,n_k \geq 0 \\ n_1+\dots+n_k=n}} X_{n_1 \dots n_k}$. Then X_n is an open subscheme of X (because it is a union of open subsets). Gluing the isomorphisms $\varphi_{n_1 \dots n_k}$'s we get an isomorphism of schemes

$$\begin{aligned}\varphi_n : \coprod_{\substack{n_1,\dots,n_k \in \mathbb{Z} \\ n_1,\dots,n_k \geq 0 \\ n_1+\dots+n_k=n}} X_{n_1 \dots n_k} = X_n \to \coprod_{\substack{n_1,\dots,n_k \in \mathbb{Z} \\ n_1,\dots,n_k \geq 0 \\ n_1+\dots+n_k=n}} \coprod_{\alpha=1}^{n_1+\dots+n_k=n} X_{n_1 \dots n_k} = \\ = \coprod_{\alpha=1}^{n} \coprod_{\substack{n_1,\dots,n_k \in \mathbb{Z} \\ n_1,\dots,n_k \geq 0 \\ n_1+\dots+n_k=n}} X_{n_1 \dots n_k} = \coprod_{\alpha=1}^{n} X_n .\end{aligned}$$

Let $p_n : \coprod_{\alpha=1}^n X_n \to X_n$ be the morphism obtained gluing the identity morphisms $\mathrm{id}_{X_n} : X_n \to X_n$. Let $n_1, \dots, n_k \in \mathbb{Z}$, $n_1, \dots, n_k \geq 0$ be such that $n_1 + \dots + n_k$.

Then $(p_n)_{|\coprod_{\alpha=1}^n X_{n_1\dots n_k}}$ is obtained by gluing the identity morphisms $(\mathrm{id}_{X_n})_{|X_{n_1\dots n_k}} = \mathrm{id}_{X_{n_1\dots n_k}}$ and so it coincides with $p_{n_1\dots n_k}$. It follows that

$$(p_n \circ \varphi_n)_{|X_{n_1\dots n_k}} = (p_n)_{|_{|\coprod_{\alpha=1}^n X_{n_1\dots n_k}}} \circ (\varphi_n)_{|X_{n_1\dots n_k}} = p_{n_1\dots n_k} \circ \varphi_{n_1\dots n_k} = f \ .$$

Since this holds for any $n_1, \dots, n_k$, we get that $p_n \circ \varphi_n = f$. Finally, we have that

$$X = \coprod_{\substack{n_1,\dots,n_k \in \mathbb{Z} \\ n_1,\dots,n_k \geq 0}} X_{n_1\dots n_k} = \coprod_{\substack{n\in\mathbb{Z} \\ n\geq 0}} \coprod_{\substack{n_1,\dots,n_k \in \mathbb{Z} \\ n_1,\dots,n_k \geq 0 \\ n_1+\dots+n_k=n}} X_{n_1\dots n_k} = \coprod_{\substack{n\in\mathbb{Z} \\ n\geq 0}} X_n \ .$$

Hence f is totally split. ☐

Lemma 2.2.40. *Let $(X_i)_{i\in I}$, $(Y_i)_{i\in I}$ be two collections of schemes and define $X := \coprod_{i\in I} X_i$, $Y := \coprod_{i\in I} Y_i$ (disjoint union of schemes). Moreover, let $f_i : X_i \to Y_i$ be a totally split morphism of schemes for every $i \in I$. If $f : X \to Y$ is the induced morphism of schemes, then f is totally split.*

Proof. Let $i \in I$. Since f_i is totally split, we can write $X_i = \coprod_{\substack{n\in\mathbb{Z} \\ n\geq 0}} X_{in}$ for some schemes $X_{i0}, X_{i1}, \dots$ such that, for any $n \in \mathbb{Z}$, $n \geq 0$, there exists an isomorphism of schemes $\varphi_{in} : f_i^{-1}(X_{in}) \to \coprod_{\alpha=1}^n X_{in}$ such that $p_{in} \circ \varphi_{in} = f_i$, where $p_{in} : \coprod_{\alpha=1}^n X_{in} \to X_{in}$ is obtained by gluing the identity morphisms $\mathrm{id}_{X_{in}} : X_{in} \to X_{in}$. Then we have that

$$X = \coprod_{i\in I} X_i = \coprod_{i\in I} \coprod_{\substack{n\in\mathbb{Z} \\ n\geq 0}} X_{in} = \coprod_{\substack{n\in\mathbb{Z} \\ n\geq 0}} \coprod_{i\in I} X_{in} \ .$$

For any $n \in \mathbb{Z}$, $n \geq 0$, define $X_n := \coprod_{i\in I} X_{in}$, so that $X = \coprod_{\substack{n\in\mathbb{Z} \\ n\geq 0}} X_n$. Fix $n \in \mathbb{Z}$, $n \geq 0$. We have that $f^{-1}(X_n) = f^{-1}\left(\coprod_{i\in I} X_{in}\right) = \coprod_{i\in I} f^{-1}(X_{in})$. Then we can glue the morphisms of schemes $\varphi_{in} : f^{-1}(X_{in}) \to \coprod_{\alpha=1}^n X_{in}$ to get a morphism of schemes

$$\varphi_n : f^{-1}(X_n) = \coprod_{i\in I} f^{-1}(X_{in}) \to \coprod_{i\in I} \coprod_{\alpha=1}^{n} X_{in} = \coprod_{\alpha=1}^{n} \coprod_{i\in I} X_{in} = \coprod_{\alpha=1}^{n} X_n \ .$$

Since φ_{in} is an isomorphism for each $i \in I$, we can consider the inverses φ_{in}^{-1}'s. Gluing them, we get a morphism of schemes $\varphi'_n : \coprod_{i\in I} \coprod_{\alpha=1}^n X_{in} = \coprod_{\alpha=1}^n X_n \to \coprod_{i\in I} f^{-1}(X_{in}) = f^{-1}(X_n)$. We have that $(\varphi'_n \circ \varphi_n)_{|f^{-1}(X_{in})} = (\varphi'_n)_{|\coprod_{\alpha=1}^n X_{in}} \circ (\varphi_n)_{|f^{-1}(X_n)} = \varphi_{in}^{-1} \circ \varphi_{in} = \mathrm{id}_{f^{-1}(X_{in})} = (\mathrm{id}_{f^{-1}(X_n)})_{|f^{-1}(X_{in})}$ for any $n \in \mathbb{Z}$, $n \geq 0$. So $\varphi'_n \circ \varphi_n = \mathrm{id}_{f^{-1}(X_n)}$. Analogously, one can show that $\varphi_n \circ \varphi'_n = \mathrm{id}_{\coprod_{\alpha=1}^n X_n}$. So φ_n is an isomorphism. Let $p_n : \coprod_{\alpha=1}^n X_n \to X_n$ be the morphism obtained by gluing the identity morphisms $\mathrm{id}_{X_n} : X_n \to X_n$. As above, we have that $\coprod_{\alpha=1}^n X_n = \coprod_{i\in I} \coprod_{\alpha=1}^n X_{in}$. Let $i \in I$. We have that $(p_n)_{|X_{in}} = (\mathrm{id}_{X_n})_{|X_{in}} = \mathrm{id}_{X_{in}}$ and so, recalling the definition of p_{in}, we get that $(p_n)_{|\coprod_{\alpha=1}^n X_{in}} = p_{in}$. Then

$$(p_n \circ \varphi_n)_{|f^{-1}(X_{in})} = (p_n)_{|\coprod_{\alpha=1}^n X_{in}} \circ (\varphi_n)_{|f^{-1}(X_{in})} = p_{in} \circ \varphi_{in} = f_i = f_{|f^{-1}(X_{in})} \ .$$

Since this holds for any $i \in I$, we have that $p_n \circ \varphi_n = f$. Hence f is totally split. ☐

Lemma 2.2.41. *Let X, Y and W be schemes. Let $f : Y \to X$ be a totally split morphism and $g : W \to X$ any morphism of schemes. Consider the fibred product $Y \times_X W$, with the projections $p_1 : Y \times_X W \to Y$ and $p_2 : Y \times_X W \to W$. Then p_2 is totally split.*

Proof. Since f is totally split, there exist some schemes $X_0, X_1, \dots$ such that $X = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n$ and, for any $n \in \mathbb{Z}$, $n \geq 0$, there exists an isomorphism of schemes $\varphi_n : f^{-1}(X_n) \to \coprod_{i=1}^n X_n$ such that $\pi_n \circ \varphi_n = f$, where $\pi_n : \coprod_{i=1}^n X_n \to X_n$ is obtained by gluing the identity morphisms $\mathrm{id}_{X_n} : X_n \to X_n$. For any $n \in \mathbb{Z}$, $n \geq 0$, define $W_n := g^{-1}(X_n)$. Then, since g is a morphism of schemes, we have that

$$W = g^{-1}(X) = g^{-1}\left(\coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n\right) = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} g^{-1}(X_n) = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} W_n \ ,$$

as schemes. Fix $n \in \mathbb{Z}$, $n \geq 0$. We have that $p_2^{-1}(W_n) = p_2^{-1}(g^{-1}(X_n)) = f^{-1}(X_n) \times_{X_n} g^{-1}(X_n) = f^{-1}(X_n) \times_{X_n} W_n$, with the obvious projections (this can be checked as in the proof of lemma 2.2.34). Consider the disjoint union $\coprod_{i=1}^n W_n$ and let $q_n : \coprod_{i=1}^n W_n \to W_n$ be the morphism obtained by gluing the identity morphisms $\mathrm{id}_{W_n} : W_n \to W_n$. Moreover, let $q'_n : \coprod_{i=1}^n W_n \to \coprod_{i=1}^n X_n$ be the morphism obtained by gluing n-times the morphism $g : W_n = g^{-1}(X_n) \to X_n$. Then $g \circ q_n = \pi_n \circ q'_n$. Moreover, let Z be a scheme with two morphisms $h_1 : Z \to \coprod_{i=1}^n X_n$ and $h_2 : Z \to W_n$ such that $g \circ h_2 = \pi_n \circ h_1$. For any $i = 1, \dots, n$, let Z_i be the preimage under h_1 of the i-th copy of X_n. Then

$$Z = h_1^{-1}\left(\coprod_{i=1}^n X_n\right) = \coprod_{i=1}^n h_1^{-1}(X_n) = \coprod_{i=1}^n Z_i \ .$$

For any $i = 1, \dots, n$, consider the restriction $h_i := (h_2)_{|Z_i} : Z_i \to W_n$. Let $h : \coprod_{i=1}^n Z_i \to \coprod_{i=1}^n W_n$ be the morphism of schemes obtained by gluing the h_i's. For any $j = 1, \dots, n$, let $\iota_j : X_n \to \coprod_{i=1}^n X_n$ and $\iota'_j : W_n \to \coprod_i^n W_n$ be the j-th canonical inclusions, so that $q_n \circ \iota'_j = \mathrm{id}_{W_n}$, $q'_n \circ \iota'_j = \iota_j \circ g$ and $h_{|Z_j} = \iota'_j \circ h_j$. Then, for any $i = 1, \dots, n$,we have that

$$(q_n \circ h)_{|Z_i} = q_n \circ h_{|Z_i} = q_n \circ \iota'_i \circ h_i = \mathrm{id}_{W_n} \circ (h_2)_{|Z_i} = (h_2)_{|Z_i}$$

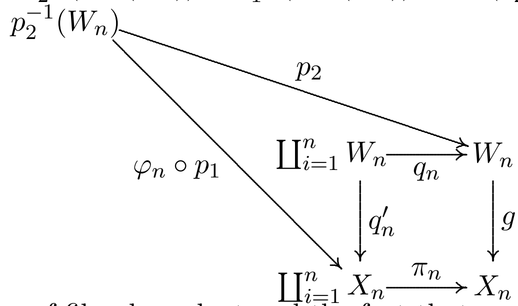
and

$$\begin{aligned}(q'_n \circ h)_{|Z_i} = q'_n \circ h_{|Z_i} = q'_n \circ \iota'_i \circ h_i = \iota_i \circ g \circ (h_2)_{|Z_i} = \iota_i \circ (g \circ h_2)_{|Z_i} = \\ = \iota_i \circ (\pi_n \circ h_1)_{|Z_i} = \iota_i \circ \pi_n \circ (h_1)_{|Z_i} = \mathrm{id}_{\coprod_{i=1}^n X_n} \circ (h_1)_{|Z_i} = (h_1)_{|Z_i}\end{aligned}$$

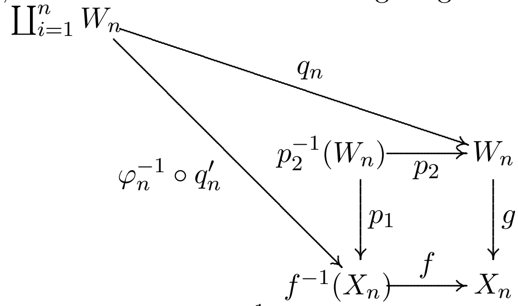
(by definition, the restriction of $\iota_i \circ \pi_n$ to the i-th component of $\coprod_{i=1}^n X_i$ coincides with the restriction of the identity). Since this holds for any $i = 1, \dots, n$, it follows that $q_n \circ h = h_2$ and $q'_n \circ h = h_1$. On the other hand, if $\widetilde{h} : Z \to \coprod_{i=1}^n W_n$ is another morphism of schemes such that $q_n \circ \widetilde{h} = h_2$ and $q'_n \circ \widetilde{h} = h_1$, then for any $i = 1, \dots, n$ we have that $q'_n(\widetilde{h}(Z_i)) = h_1(Z_i)$ is contained in the i-th copy of X_n, so $\widetilde{h}(Z_i)$ is contained in the preimage under q'_n of the i-th copy of X_n. This preimage is, by definition of q'_n, the i-th copy of W_n inside $\coprod_{i=1}^n W_n$. Then

$$\widetilde{h}_{|Z_i} = \iota'_i \circ q_n \circ \widetilde{h}_{|Z_i} = \iota'_i \circ (q_n \circ \widetilde{h})_{|Z_i} = \iota'_i \circ (h_2)_{|Z_i} = \iota'_i \circ h_i = h_{|Z_i} .$$

Since this holds for any $i = 1, \ldots, n$, it follows that $\widetilde{h} = h$. This shows that $\coprod_{i=1}^n W_n$, together with the morphisms $q'_n : \coprod_{i=1}^n W_n \to \coprod_{i=1}^n X_n$ and $q_n : \coprod_{i=1}^n W_n \to W_n$, is the fibred product of $\coprod_{i=1}^n X_n$ and W_n over X_n. Consider now the following diagram (recall that $p_2^{-1}(W_n) = p_2^{-1}(g^{-1}(X_n)) = p_1^{-1}(f^{-1}(X_n))$, so $p_1(p_2^{-1}(W_n)) \subseteq f^{-1}(X_n)$).



Applying the definition of fibred product and the fact that $\pi_n \circ \varphi_n = f$, we get that $\pi_n \circ \varphi_n \circ p_1 = f \circ p_1 = g \circ p_2$. So the diagram is commutative and, since $\coprod_{i=1}^n W_n = (\coprod_{i=1}^n X_n) \times_{X_n} W_n$, there exists a unique morphism $\psi_n : p_2^{-1}(W_n) \to \coprod_{i=1}^n W_n$ such that $q'_n \circ \psi_n = \varphi_n \circ p_1$ and $q_n \circ \psi_n = p_2$. We claim that ψ_n is an isomorphism. Since φ_n is an isomorphism, we can consider the following diagram.



Since $\pi_n \circ \varphi_n = f$, we have that $f \circ \varphi_n^{-1} = \pi_n$. Recalling that $\pi_n \circ q'_n = g \circ q_n$, we get that $f \circ \varphi_n^{-1} \circ q'_n = \pi_n \circ q'_n = g \circ q_n$. So the diagram is commutative and, since $p_2^{-1}(W_n) = f^{-1}(X_n) \times_{X_n} W_n$, there exists a unique morphism $\psi'_n : \coprod_{i=1}^n W_n \to p_2^{-1}(W_n)$ such that $p_1 \circ \psi'_n = \varphi_n^{-1} \circ q'_n$ and $p_2 \circ \psi'_n = q_n$. We have that

$$p_1 \circ (\psi'_n \circ \psi_n) = \varphi_n^{-1} \circ q'_n \circ \psi_n = \varphi_n^{-1} \circ \varphi_n \circ p_1 = p_1 = p_1 \circ \mathrm{id}_{p_2^{-1}(W_n)}$$

and

$$p_2 \circ (\psi'_n \circ \psi_n) = q_n \circ \psi_n = p_2 = p_2 \circ \mathrm{id}_{p_2^{-1}(W_n)} .$$

By uniqueness in the universal property of the fibred product, this implies that $\psi'_n \circ \psi_n = \mathrm{id}_{p_2^{-1}(W_n)}$. On the other hand,

$$q'_n \circ (\psi_n \circ \psi'_n) = \varphi_n \circ p_1 \circ \psi'_n = \varphi_n \circ \varphi_n^{-1} \circ q'_n = q'_n = q'_n \circ \mathrm{id}_{\coprod_{i=1}^n W_n}$$

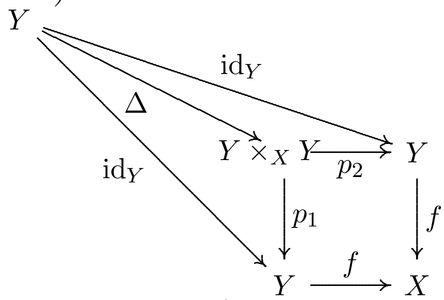
and

$$q_n \circ (\psi_n \circ \psi'_n) = p_2 \circ \psi'_n = q_n = q_n \circ \mathrm{id}_{\coprod_{i=1}^n W_n} .$$

By uniqueness in the universal property of the fibred product, this implies that $\psi_n \circ \psi'_n = \mathrm{id}_{\coprod_{i=1}^n W_n}$. So ψ_n and ψ'_n are inverse to each other. In particular, ψ_n is an isomorphism of schemes. We already know that $q_n \circ \psi_n = p_2$. Since this construction holds for any $n \in \mathbb{Z}$, $n \geq 0$, we have that p_2 is totally split. □

The following lemma is a preparation for the proof of a proposition that will be a key tool in our proof that $\mathbf{FEt}_X$ is a Galois category if X is connected.

Lemma 2.2.42. *Let X, Y be schemes and $f : Y \to X$ a finite étale morphism. Consider the fibred product $Y \times_X Y$, with projections $p_1 : Y \times_X Y \to Y$ and $p_2 : Y \times_X Y \to Y$. Let $\Delta : Y \to Y \times_X Y$ be the unique morphism such that the following diagram is commutative (existence and uniqueness of Δ follow from the universal property of the fibred product).*



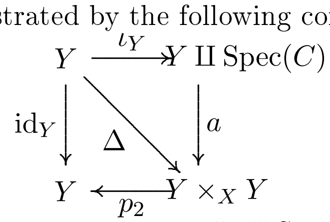
Then $\Delta(Y)$ (the set-theoretic image of Δ) is both open and closed in $Y \times_X Y$ and $\Delta : Y \to \Delta(Y)$ is an isomorphism of schemes.

Proof. First of all, we prove this in the case when $X = \mathrm{Spec}(A)$ is affine. Since f is finite étale, by lemma 2.2.10(4) we have that $f^{-1}(X)$ is affine and equal to $\mathrm{Spec}(B)$, where B is a projective separable A-algebra. Then $Y \times_X Y = \mathrm{Spec}(B) \times_{\mathrm{Spec}(A)} \mathrm{Spec}(B) = \mathrm{Spec}(B \otimes_A B)$ (see the proof of theorem 3.3 in chapter II of [4]). Consider on $B \otimes_A B$ the B-algebra structure induced by the morphism of schemes $p_2 : Y \otimes_X Y = \mathrm{Spec}(B \otimes_A B) \to Y = \mathrm{Spec}(B)$, i.e. the B-algebra structure via the second factor. The morphism of schemes $\Delta : Y = \mathrm{Spec}(B) \to Y \times_X Y = \mathrm{Spec}(B \otimes_A B)$ corresponds to a ring homomorphism $\Delta^\# : B \otimes_A B \to B$, which is also a B-algebra homomorphism, because $p_2 \circ \Delta = \mathrm{id}_Y$. Since $p_1 \circ \Delta = \mathrm{id}_Y = p_2 \circ \Delta$, we have that $\Delta^\# \circ p_1^\# = \mathrm{id}_B = \Delta^\# \circ p_2^\#$. Then, for any $x, y \in B$, we have that

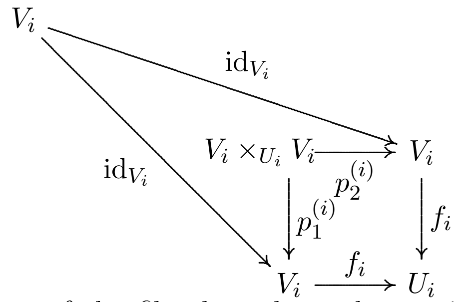
$$\begin{aligned}\Delta^\#(x \otimes y) = \Delta^\#((x \otimes 1)(1 \otimes y)) = \Delta^\#(x \otimes 1)\Delta^\#(1 \otimes y) = \\ = \Delta^\#(p_1^\#(x))\Delta^\#(p_2^\#(y)) = \mathrm{id}_B(x)\,\mathrm{id}_B(y) = xy\end{aligned}$$

(we applied the fact that $\Delta^\#$ is a ring homomorphism). So, since $\Delta^\#$ is B-linear we have that $\Delta^\# = \delta$, where δ is the map defined in proposition 2.1.75. By that proposition (which we can apply because B is a projective separable A-algebra), there exist a B-algebra C and an isomorphism of B-algebras $\alpha : B \otimes_A B \to B \times C$ such that $\delta = p_B \circ \alpha$, where $p_B : B \times C \to B$ is the canonical projection (which is a B-algebra homomorphism, in particular a ring homomorphism). Now we translate this into the language of schemes. The isomorphism α corresponds to an isomorphism of schemes $a : \mathrm{Spec}(B \times C) \to \mathrm{Spec}(B \otimes_A B) = Y \times_X Y$. As in the proof of lemma 2.2.18, we have that $\mathrm{Spec}(B \times C) = \mathrm{Spec}(B) \amalg \mathrm{Spec}(C) = Y \amalg \mathrm{Spec}(C)$.

The ring homomorphism $p_B : B \times C \to B$ corresponds to the canonical inclusion $\iota_Y : Y = \mathrm{Spec}(B) \to Y \amalg \mathrm{Spec}(C) = \mathrm{Spec}(B \times C)$. Then, since $\delta = p_B \circ \alpha$, we have that $\Delta = a \circ \iota_Y$. This is illustrated by the following commutative diagram.



We have that Y is both open and closed in $Y \amalg \mathrm{Spec}(C)$ by definition of disjoint union. Then $\Delta(Y) = a(\iota_Y(Y)) = a(Y)$ is both open and closed in $Y \times_X Y$, because a is an isomorphism of schemes (in particular, a homeomorphism). Moreover, $\iota_Y : Y \to \iota_Y(Y) = Y \subseteq Y \amalg \mathrm{Spec}(C)$ is an isomorphism of schemes and, since $a : Y \amalg \mathrm{Spec}(C) \to Y \times_X Y$ is an isomorphism of schemes, also the restriction $a_{|_Y} : Y = \iota_Y(Y) \to a(\iota_Y(Y)) = \Delta(Y)$ is an isomorphism of schemes. Then the composition $a_{|_Y} \circ \iota_Y = \Delta : Y \to \Delta(Y)$ is an isomorphism of schemes, as we wanted.
Consider now the general case (X not necessarily affine). By definition of scheme, there exists a cover of X by open affine subsets $(U_i)_{i \in I}$. Let $i \in I$ and define $V_i := f^{-1}(U_i)$. Then V_i is an open subscheme of Y. By lemma 2.2.22, the restriction $f_i := f_{|_{V_i}} : V_i = f^{-1}(U_i) \to U_i$ is finite étale. Consider the fibred product $V_i \times_{U_i} V_i$, with projections $p_1^{(i)} : V_i \times_{U_i} V_i \to V_i$ and $p_2^{(i)} : V_i \times_{U_i} V_i \to V_i$. Consider the following commutative diagram.



By the universal property of the fibred product, there exists a unique morphism $\Delta_i : V_i \to V_i \times_{U_i} V_i$ such that $p_1^{(i)} \circ \Delta_i = \mathrm{id}_{V_i} = p_2^{(i)} \circ \Delta_i$. Since U_i is affine, by what we proved above we have that $\Delta_i(V_i)$ is both open and closed in $V_i \times_{U_i} V_i$ and that $\Delta_i : V_i \to \Delta_i(V_i)$ is an isomorphism of schemes. As in the proof of theorem 3.3 in chapter II of [4], we have that $Y \times_X Y = \bigcup_{i \in I}(V_i \times_{U_i} V_i)$ and $V_i \times_{U_i} V_i$ is open in $Y \times_X Y$ for every $i \in I$. Moreover, $p_1^{(i)} = (p_1)_{|_{V_i \times_{U_i} V_i}}$ and $p_2^{(i)} = (p_2)_{|_{V_i \times_{U_i} V_i}}$, for every $i \in I$. Fix $i \in I$. Since $V_i \times_{U_i} V_i$ is an open subscheme of $Y \times_X Y$, we can consider Δ_i as a morphism $V_i \to Y \times_X Y$. We have that

$$p_1 \circ \Delta_i = p_1^{(i)} \circ \Delta_i = \mathrm{id}_{V_i} = (\mathrm{id}_Y)_{|_{V_i}} = (p_1 \circ \Delta)_{|_{V_i}} = p_1 \circ \Delta_{|_{V_i}}$$

and

$$p_2 \circ \Delta_i = p_2^{(i)} \circ \Delta_i = \mathrm{id}_{V_i} = (\mathrm{id}_Y)_{|_{V_i}} = (p_2 \circ \Delta)_{|_{V_i}} = p_2 \circ \Delta_{|_{V_i}} .$$

Then, by uniqueness in the universal property of the fibred product, we have that $\Delta_i = \Delta_{|_{V_i}}$. It follows that $\Delta(V_i) = \Delta_i(V_i)$, which is both open and closed in $V_i \times_{U_i} V_i$. Since $V_i \times_{U_i} V_i$ is open in $Y \times_X Y$, we have that $\Delta(V_i)$ is open in $Y \times_X Y$. Since this

holds for any $i \in I$ and $Y = \bigcup_{i \in I} V_i$, we have that $\Delta(Y) = \Delta\left(\bigcup_{i \in I} V_i\right) = \bigcup_{i \in I} \Delta(V_i)$ is open in $Y \times_X Y$, because it is a union of open subsets.
Let $i \in I$. Notice that $\Delta^{-1}(V_i \times_{U_i} V_i) = V_i$. Indeed, $\Delta(V_i) = \Delta_i(V_i) \subseteq V_i \times_{U_i} V_i$ implies that $V_i \subseteq \Delta^{-1}(V_i \times_{U_i} V_i)$. Conversely, if $y \in \Delta^{-1}(V_i \times_{U_i} V_i)$, we have that $\Delta(y) \in V_i \times_{U_i} V_i$ and then, since $p_1 \circ \Delta = \mathrm{id}_Y$ and $(p_1)_{|V_i \times_{U_i} V_i} = p_1^{(i)}$, we get that $y = \mathrm{id}_Y(y) = p_1(\Delta(y)) = p_1^{(i)}(\Delta(y)) \in V_i$. This shows that $\Delta^{-1}(V_i \times_{U_i} V_i) = V_i$. Then $\Delta(Y) \cap (V_i \times_{U_i} V_i) = \Delta(\Delta^{-1}(V_i \times_{U_i} V_i)) = \Delta(V_i)$. It follows that

$$(Y \times_X Y)\backslash\Delta(Y) = \left(\bigcup_{i \in I}(V_i \times_{U_i} V_i)\right)\backslash\Delta(Y) = \bigcup_{i \in I}((V_i \times_{U_i} V_i)\backslash\Delta(Y)) =$$
$$= \bigcup_{i \in I}((V_i \times_{U_i} V_i)\backslash(\Delta(Y) \cap (V_i \times_{U_i} V_i))) = \bigcup_{i \in I}((V_i \times_{U_i} V_i)\backslash\Delta(V_i)) .$$

For any $i \in I$, since $\Delta(V_i)$ is closed in $V_i \times_{U_i} V_i$, we have that $(V_i \times_{U_i} V_i)\backslash\Delta(V_i)$ is open in $V_i \times_{U_i} V_i$ and then also in $Y \times_X Y$, because $V_i \times_{U_i} V_i$ is open in $Y \times_X Y$. So $(Y \times_X Y)\backslash\Delta(Y) = \bigcup_{i \in I}((V_i \times_{U_i} V_i)\backslash\Delta(V_i))$ is open in $Y \times_X Y$, because it is a union of open subsets. So $\Delta(V_i)$ is closed in $Y \times_X Y$.
Finally, for any $i \in I$ we know that $\Delta_i : V_i \to \Delta_i(V_i)$ is an isomorphism of schemes and so we can consider the inverse morphism $\Delta_i^{-1} : \Delta_i(V_i) = \Delta(V_i) \to V_i$. These morphisms agree on the overlaps. Indeed, for any $i, j \in I$ we have that $\Delta^{-1}(\Delta(V_i) \cap \Delta(V_j)) = \Delta^{-1}(\Delta(V_i)) \cap \Delta^{-1}(\Delta(V_j)) = V_i \cap V_j$ (the last equality follows from the fact that $\Delta^{-1}(\Delta(V_k)) = \Delta^{-1}(\Delta(\Delta^{-1}(V_k \times_{U_k} V_k))) = \Delta^{-1}(V_k \times_{U_k} V_k) = V_k$ for any $k \in I$) and so

$$(\Delta_i^{-1})_{|\Delta(V_i)\cap\Delta(V_j)} = \left(\left(\Delta_{|V_i}\right)^{-1}\right)_{|\Delta(V_i)\cap\Delta(V_j)} = \left(\left(\Delta_{|V_i}\right)_{|V_i \cap V_j}\right)^{-1} = (\Delta_{|V_i \cap V_j})^{-1} =$$
$$= \left(\left(\Delta_{|V_j}\right)_{|V_i \cap V_j}\right)^{-1} = \left(\left(\Delta_{|V_j}\right)^{-1}\right)_{|\Delta(V_i)\cap\Delta(V_j)} = (\Delta_j^{-1})_{|\Delta(V_i)\cap\Delta(V_j)} .$$

Then we can glue the morphisms Δ_i^{-1}'s and a get a morphism

$$\Delta' : \bigcup_{i \in I} \Delta(V_i) = \Delta(Y) \to \bigcup_{i \in I} V_i = Y .$$

We have that $\Delta : Y \to \Delta(Y)$ and $\Delta' : \Delta(Y) \to Y$ are inverse to each other, because this is true considering the restrictions to V_i and $\Delta(V_i)$, for any $i \in I$. Hence $\Delta : Y \to \Delta(Y)$ is an isomorphism of schemes. □

Proposition 2.2.43. *Let X, Y be schemes and $f : Y \to X$ a morphism of schemes. Then f is finite étale if and only if f is affine and there exist a scheme W and a surjective, finite and locally free morphism of schemes $g : W \to X$ such that the projection $p_2 : Y \times_X W \to W$ is totally split.*

Proof. Assume that f is affine and that there exist a scheme W and a surjective, finite and locally free morphism of schemes $g : W \to X$ such that the projection

$p_2 : Y \times_X W \to W$ is totally split. By lemma 2.2.37, we have that p_2 is finite étale. Then, by lemma 2.2.34, f is finite étale.
Conversely, assume that f is finite étale. We know that in this case f is affine (remark 2.2.4). So we have to show the existence of W and g with the desired properties. We assume firstly that f has constant degree and we prove the claim by induction on $n := [Y : X]$. If $n = 0$, then $Y = \emptyset$, by lemma 2.2.15(1). Define $W := X$ and $g := \mathrm{id}_X$. Then g is clearly surjective. Moreover, g is totally split (example 2.2.36) and so it is finite étale by lemma 2.2.37. In particular, g is finite and locally free. So the requirements about g are satisfied. Consider the fibred product $Y \times_X W$, with projections $p_1 : Y \times_X W \to Y$ and $p_2 : Y \times_X W \to W$. Since $Y = \emptyset$ and we have the morphism $p_1 : Y \times_X W \to Y$, we must have $Y \times_X W = \emptyset$. Then $p_2 : Y \times_X W = \emptyset \to W$ is totally split (set $W_0 := W$ and $W_k := \emptyset$ for any $k \neq 0$).
Let now $n \geq 1$ and assume that the claim is true for any finite étale morphism of degree less than n. Consider the fibred product $Y \times_X Y$, with projections $q_1 : Y \times_X Y \to Y$ and $q_2 : Y \times_X Y \to Y$. Since f is finite étale, by lemma 2.2.28(4) we have that q_2 is finite étale. Moreover, by point (2) of the same lemma, we have that $[Y \times_X Y : Y](y) = [Y : X](f(y)) = n$ for any $y \in Y$. Let $\Delta : Y \to Y \times_X Y$ be the unique morphism such that $q_1 \circ \Delta = \mathrm{id}_Y = q_2 \circ \Delta$ (existence and uniqueness follow from the universal property of the fibred product). By lemma 2.2.42, we have that $\Delta(Y)$ is both open and closed in $Y \times_X Y$ and that $\Delta : Y \to \Delta(Y)$ is an isomorphism of schemes. Then $Y \times_X Y = \Delta(Y) \amalg Y'$ (disjoint union of schemes), where we defined $Y' := (Y \times_X Y) \backslash \Delta(Y)$. Define $q := (q_2)_{|\Delta(Y)} : \Delta(Y) \to Y$ and $q' := (q_2)_{|Y'} : Y' \to Y$. Since q_2 is finite étale, by lemma 2.2.18(2)-(3) we have that also q and q' are finite étale and $n = [Y \times_X Y : Y] = [\Delta(Y) : Y] + [Y' : Y]$. Since $q \circ \Delta = (q_2)_{|\Delta(Y)} \circ \Delta = q_2 \circ \Delta = \mathrm{id}_Y$ and we proved that $\Delta : Y \to \Delta(Y)$ is an isomorphism, we have that $q = \Delta^{-1} : \Delta(Y) \to Y$ is an isomorphism. Then, by lemma 2.2.15(2), we have that $[\Delta(Y) : Y] = 1$. So $[Y' : Y] = n - 1$. Applying the induction hypothesis, we have that there exist a scheme W and a surjective, finite and locally free morphism of schemes $g' : W \to Y$ such that the projection $p'_2 : Y' \times_Y W \to W$ is totally split. Define $g := f \circ g' : W \to X$. Since f is finite étale, it is in particular finite and locally free. Then, by lemma 2.2.30 we have that g is finite and locally free. Moreover, since $[Y : X] = n \geq 1$, by lemma 2.2.15(3) we have that f is surjective. Then g is surjective, because it is a composition of surjective maps. So g satisfies the required properties. Consider the fibred product $\Delta(Y) \times_Y W$, with projections $p''_1 : \Delta(Y) \times_Y W \to \Delta(Y)$ and $p''_2 : \Delta(Y) \times_Y W \to W$. Consider the morphisms $\Delta \circ g' : W \to \Delta(Y)$ and $\mathrm{id}_W : W \to W$. We have that $q \circ (\Delta \circ g') = (\Delta^{-1} \circ \Delta) \circ g' = g' = g' \circ \mathrm{id}_W$, so by the universal property of the fibred product there exists a unique morphism $\vartheta : W \to \Delta(Y) \times_Y W$ such that $p''_1 \circ \vartheta = \Delta \circ g'$ and $p''_2 \circ \vartheta = \mathrm{id}_W$. Consider $\vartheta \circ p''_2 : \Delta(Y) \times_Y W \to \Delta(Y) \times_Y W$. We have that

$$p''_1 \circ (\vartheta \circ p''_2) = \Delta \circ g' \circ p''_2 = \Delta \circ q \circ p''_1 = \Delta \circ \Delta^{-1} \circ p''_1 = p''_1 = p''_1 \circ \mathrm{id}_{\Delta(Y) \times_Y W}$$

and

$$p''_2 \circ (\vartheta \circ p''_2) = \mathrm{id}_W \circ p''_2 = p''_2 = p''_2 \circ \mathrm{id}_{\Delta(Y) \times_Y W} \ .$$

By uniqueness in the universal property of the fibred product, it follows that $\vartheta \circ$

$p_2'' = \mathrm{id}_{\Delta(Y)\times_Y W}$. So p_2'' and ϑ are inverse to each other. This shows that p_2'' is an isomorphism of schemes. Then p_2'' is totally split, by example 2.2.36. Gluing $p_2' : Y' \times_Y W \to W$ and $p_2'' : \Delta(Y) \times_Y W \to W$, we get a morphism $p_2 : (\Delta(Y) \times_Y W) \amalg (Y' \times_Y W) \to W$, which is totally split by lemma 2.2.39. Let $p_1' : Y' \times_Y W \to Y'$ be the first projection. Then we can glue p_1' with $p_1'' : \Delta(Y) \times_Y W \to \Delta(Y)$ and get a morphism $p_1 : (\Delta(Y) \times_Y W) \amalg (Y' \times_Y W) \to \Delta(Y) \amalg Y' = Y \times_X Y$. We claim that $(\Delta(Y) \times_Y W) \amalg (Y' \times_Y W)$, together with the morphisms $q_1 \circ p_1 : (\Delta(Y) \times_Y W) \amalg (Y' \times_Y W) \to Y$ and $p_2 : (\Delta(Y) \times_Y W) \amalg (Y' \times_Y W) \to W$ is the fibred product of Y and W over X. First of all, notice that

$$\begin{aligned}(q_2 \circ p_1)_{|\Delta(Y)\times_Y W} &= (q_2)_{|\Delta(Y)} \circ (p_1)_{|\Delta(Y)\times_Y W} = q \circ p_1'' = \\ &= g' \circ p_2'' = g' \circ (p_2)_{|\Delta(Y)\times_Y W} = (g' \circ p_2)_{|\Delta(Y)\times_Y W}\end{aligned}$$

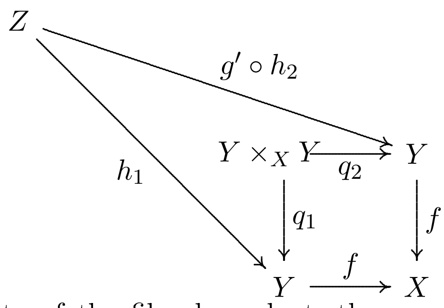
and

$$\begin{aligned}(q_2 \circ p_1)_{|Y'\times_Y W} &= (q_2)_{|Y'} \circ (p_1)_{|Y'\times_Y W} = q' \circ p_1' = \\ &= g' \circ p_2' = g' \circ (p_2)_{|Y'\times_Y W} = (g' \circ p_2)_{|Y'\times_Y W} .\end{aligned}$$

Then $q_2 \circ p_1 = g' \circ p_2$. Recall now that $f \circ q_1 = f \circ q_2$, by definition of fibred product. Then

$$f \circ (q_1 \circ p_1) = f \circ q_2 \circ p_1 = f \circ g' \circ p_2 = g \circ p_2 .$$

Let now Z be a scheme with morphisms $h_1 : Z \to Y$ and $h_2 : Z \to W$ such that $f \circ h_1 = g \circ h_2$. Since $g = f \circ g'$, this means that $f \circ h_1 = f \circ g' \circ h_2$. Consider then the following diagram.



By the universal property of the fibred product, there exists a unique morphism $\eta : Z \to Y \times_X Y = \Delta(Y) \amalg Y'$ such that $q_1 \circ \eta = h_1$ and $q_2 \circ \eta = g' \circ h_2$. Define $Z' := \eta^{-1}(Y')$ and $Z'' := \eta^{-1}(\Delta(Y))$. Then Z' and Z'' are open subschemes of Z and we have $Z = \eta^{-1}(\Delta(Y) \amalg Y') = \eta^{-1}(\Delta(Y)) \amalg \eta^{-1}(Y') = Z'' \amalg Z'$. Let moreover $\eta' := \eta_{|Z'} : Z' = \eta^{-1}(Y') \to Y'$, $\eta'' := \eta_{|Z''} : Z'' = \eta^{-1}(\Delta(Y)) \to \Delta(Y)$, $h_2' := (h_2)_{|Z'} : Z' \to W$ and $h_2'' := (h_2)_{|Z''} : Z'' \to W$. We have that

$$q' \circ \eta' = (q_2)_{|Y'} \circ \eta_{|Z'} = (q_2 \circ \eta)_{|Z'} = (g' \circ h_2)_{|Z'} = g' \circ (h_2)_{|Z'} = g' \circ h_2' .$$

So, by the universal property of the fibred product, there exists a unique morphism $h' : Z' \to Y' \times_Y W$ such that $p_1' \circ h' = \eta'$ and $p_2' \circ h' = h_2'$. Analogously, we have that

$$q \circ \eta'' = (q_2)_{|\Delta(Y)} \circ \eta_{|Z''} = (q_2 \circ \eta)_{|Z''} = (g' \circ h_2)_{|Z''} = g' \circ (h_2)_{|Z''} = g' \circ h_2'' .$$

So, by the universal property of the fibred product, there exists a unique morphism $h'' : Z'' \to \Delta(Y) \times_Y W$ such that $p_1'' \circ h'' = \eta''$ and $p_2'' \circ h'' = h_2''$. Gluing h' and h'', we get a morphism $h : Z'' \amalg Z' = Z \to (\Delta(Y) \times_Y W) \amalg (Y' \times_Y W)$. We have that

$$(p_1 \circ h)_{|Z'} = (p_1)_{|Y' \times_Y W} \circ h_{|Z'} = p_1' \circ h' = \eta' = \eta_{|Z'}$$

and

$$(p_1 \circ h)_{|Z''} = (p_1)_{|\Delta(Y) \times_Y W} \circ h_{|Z''} = p_1'' \circ h'' = \eta'' = \eta_{|Z''} .$$

So $p_1 \circ h = \eta$. It follows that $(q_1 \circ p_1) \circ h = q_1 \circ \eta = h_1$. We have also that

$$(p_2 \circ h)_{|Z'} = (p_2)_{|Y' \times_Y W} \circ h_{|Z'} = p_2' \circ h' = h_2' = (h_2)_{|Z'}$$

and

$$(p_2 \circ h)_{|Z''} = (p_2)_{|\Delta(Y) \times_Y W} \circ h_{|Z''} = p_2'' \circ h'' = h_2'' = (h_2)_{|Z''} .$$

So $p_2 \circ h = h_2$. Let $\widetilde{h} : Z \to (\Delta(Y) \times_Y W) \amalg (Y' \times_Y W)$ be another morphism of schemes such that $(q_1 \circ p_1) \circ \widetilde{h} = h_1$ and $p_2 \circ \widetilde{h} = h_2$. We have that $q_1 \circ (p_1 \circ \widetilde{h}) = (q_1 \circ p_1) \circ \widetilde{h} = h_1$ and $q_2 \circ (p_1 \circ \widetilde{h}) = g' \circ p_2 \circ \widetilde{h} = g' \circ h_2$ (recall that $q_2 \circ p_1 = g' \circ p_2$). This implies that $p_1 \circ \widetilde{h} = \eta$, by uniqueness of η. Then we have that $Z' = \eta^{-1}(Y') = (p_1 \circ \widetilde{h})^{-1}(Y') = \widetilde{h}^{-1}(p_1^{-1}(Y')) \subseteq \widetilde{h}^{-1}(Y' \times_Y W)$ and so $\widetilde{h}(Z') \subseteq Y' \times_Y W$. It follows that

$$p_1' \circ \widetilde{h}_{|Z'} = (p_1)_{|Y' \times_Y W} \circ \widetilde{h}_{|Z'} = \left(p_1 \circ \widetilde{h}\right)_{|Z'} = \eta_{|Z'} = \eta'$$

and

$$p_2' \circ \widetilde{h}_{|Z'} = (p_2)_{|Y' \times_Y W} \circ \widetilde{h}_{|Z'} = \left(p_2 \circ \widetilde{h}\right)_{|Z'} = (h_2)_{|Z'} = h_2' .$$

By uniqueness of h', it follows that $\widetilde{h}_{|Z'} = h' = h_{|Z'}$. Analogously, one can show that $\widetilde{h}_{|Z''} = h'' = h_{|Z''}$. So $\widetilde{h} = h$. This proves that $(\Delta(Y) \times_Y W) \amalg (Y' \times_Y W) = Y \times_X W$, with projections $q_1 \circ p_1 : (\Delta(Y) \times_Y W) \amalg (Y' \times_Y W) \to Y$ and $p_2 : (\Delta(Y) \times_Y W) \amalg (Y' \times_Y W) \to W$. We know that p_2 is totally split and so all the requirements are satisfied.

So the claim is true for any finite étale morphism of constant degree. Finally, let f be an arbitrary finite étale morphism. For any $n \in \mathbb{Z}$, $n \geq 0$, define

$$X_n := \{x \in \mathrm{sp}(X) \mid [Y : X](x) = n\} = [Y : X]^{-1}(\{n\}) ,$$

which is open in X because $\{n\}$ is open in $\mathbb{Z}$ (which has the discrete topology) and $[Y : X] : \mathrm{sp}(X) \to \mathbb{Z}$ is continuous. Then, for any $n \in \mathbb{Z}$, $n \geq 0$, we have that X_n is an open subscheme of X. So we can write $X = \coprod_{\substack{n \in \mathbb{Z} \\ n \geq 0}} X_n$. It follows that $Y = f^{-1}(X) = f^{-1}\left(\coprod_{\substack{n \in \mathbb{Z} \\ n \geq 0}} X_n\right) = \coprod_{\substack{n \in \mathbb{Z} \\ n \geq 0}} f^{-1}(X_n) = \coprod_{\substack{n \in \mathbb{Z} \\ n \geq 0}} Y_n$, where we defined $Y_n := f^{-1}(X_n)$ for any $n \in \mathbb{Z}$, $n \geq 0$. Fix $n \in \mathbb{N}$, $n \geq 0$. By corollary 2.2.24, we have that $f_n := f_{|Y_n} : Y_n \to X_n$ is finite étale and $[Y_n : X_n](x) = [Y : X](x) = n$ for any $x \in \mathrm{sp}(X_n)$. So f_n has constant rank and, by what we proved above, there exist a scheme W_n and a surjective, finite and locally free morphism of schemes $g_n : W_n \to X_n$ such that the projection $p_2^{(n)} : Y_n \times_{X_n} W_n \to W_n$ is totally split.

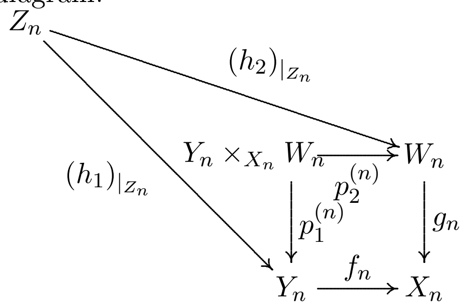
Denote by $p_1^{(n)} : Y_n \times_{X_n} W_n \to Y_n$ the first projection (then $f_n \circ p_1^{(n)} = g_n \circ p_2^{(n)}$). Define $W := \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} W_n$ and let $g : W = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} W_n \to X = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n$ be the morphism of schemes obtained by gluing the g_n's. By lemma 2.2.20, g is finite and locally free, because each g_n is finite and locally free. Moreover, let $x \in \mathrm{sp}(X)$. Since $X = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n$, there exist (a unique) $n \in \mathbb{Z}$, $n \geq 0$ such that $x \in \mathrm{sp}(X_n)$. Then, since g_n is surjective, there exists $w \in \mathrm{sp}(W_n) \subseteq \mathrm{sp}(W)$ such that $x = g_n(w) = g(w)$. This shows that g is surjective. So g satisfies the required properties. Consider now the sum $\coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}}(Y_n \times_{X_n} W_n)$. Gluing the projections $p_1^{(n)}$'s and $p_2^{(n)}$'s, we get morphisms of schemes $p_1 : \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}}(Y_n \times_{X_n} W_n) \to \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} Y_n = Y$ and $p_2 : \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}}(Y_n \times_{X_n} W_n) \to \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} W_n = W$. For any $n \in \mathbb{Z}$, $n \geq 0$, we have that

$$\begin{aligned}(f \circ p_1)_{|Y_n \times_{X_n} W_n} &= f_{|Y_n} \circ (p_1)_{|Y_n \times_{X_n} W_n} = f_n \circ p_1^{(n)} = \\ &= g_n \circ p_2^{(n)} = g_{|W_n} \circ (p_2)_{|Y_n \times_{X_n} W_n} = (g \circ p_2)_{|Y_n \times_{X_n} W_n} .\end{aligned}$$

So $f \circ p_1 = g \circ p_2$. Let now Z be a scheme with two morphisms of schemes $h_1 : Z \to Y$, $h_2 : Z \to W$ such that $f \circ h_1 = g \circ h_2$. Fix $n \in \mathbb{Z}$, $n \geq 0$. Define $Z_n := h_1^{-1}(Y_n)$. Then we have that

$$\begin{aligned}Z_n = h_1^{-1}(Y_n) &= h_1^{-1}(f^{-1}(X_n)) = (f \circ h_1)^{-1}(X_n) = \\ &= (g \circ h_2)^{-1}(X_n) = h_2^{-1}(g^{-1}(X_n)) = h_2^{-1}(W_n) .\end{aligned}$$

Consider the following diagram.



We have that

$$f_n \circ (h_1)_{|Z_n} = f_{|Y_n} \circ (h_1)_{|Z_n} = (f \circ h_1)_{|Z_n} = (g \circ h_2)_{|Z_n} = g_{|W_n} \circ (h_2)_{|Z_n} = g_n \circ (h_2)_{|Z_n} .$$

So the diagram is commutative and, by the universal property of the fibred product, there exists a unique morphism of schemes $h_n : Z_n \to Y_n \times_{X_n} W_n$ such that $p_1^{(n)} \circ h_n = (h_1)_{|Z_n}$ and $p_2^{(n)} \circ h_n = (h_2)_{|Z_n}$. We have that $Z = h_1^{-1}(Y) = h_1^{-1}\left(\coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} Y_n\right) = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} h_1^{-1}(Y_n) = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} Z_n$. So we can glue the morphisms h_n's and get a morphism of schemes $h : Z \to \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}}(Y_n \times_{X_n} W_n)$. For any $n \in \mathbb{Z}$, $n \geq 0$, we have that

$$(p_1 \circ h)_{|Z_n} = (p_1)_{|Y_n \times_{X_n} W_n} \circ h_{|Z_n} = p_1^{(n)} \circ h_n = (h_1)_{|Z_n}$$

and
$$(p_2 \circ h)_{|Z_n} = (p_2)_{|Y_n \times_{X_n} W_n} \circ h_{|Z_n} = p_2^{(n)} \circ h_n = (h_2)_{|Z_n} .$$

So $p_1 \circ h = h_1$ and $p_2 \circ h = h_2$. Let $\widetilde{h} : Z \to \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} (Y_n \times_{X_n} W_n)$ be a morphism of schemes such that $p_1 \circ \widetilde{h} = h_1$ and $p_2 \circ \widetilde{h} = h_2$ and $n \in \mathbb{Z}$, $n \geq 0$. We have that $Z_n = h_1^{-1}(Y_n) = (p_1 \circ \widetilde{h})^{-1}(Y_n) = \widetilde{h}^{-1}(p_1^{-1}(Y_n)) \subseteq \widetilde{h}^{-1}(Y_n \times_{X_n} W_n)$ and so $\widetilde{h}(Z_n) \subseteq Y_n \times_{X_n} W_n$. Then
$$p_1^{(n)} \circ \widetilde{h}_{|Z_n} = (p_1)_{|Y_n \times_{X_n} W_n} \circ \widetilde{h}_{|Z_n} = (p_1 \circ \widetilde{h})_{|Z_n} = (h_1)_{|Z_n}$$
and
$$p_2^{(n)} \circ \widetilde{h}_{|Z_n} = (p_2)_{|Y_n \times_{X_n} W_n} \circ \widetilde{h}_{|Z_n} = (p_2 \circ \widetilde{h})_{|Z_n} = (h_2)_{|Z_n} .$$

This implies that $\widetilde{h}_{|Z_n} = h_n = h_{|Z_n}$ and, since this holds for any $n \in \mathbb{Z}$, $n \geq 0$, we get that $\widetilde{h} = h$. This proves that $\coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} (Y_n \times_{X_n} W_n)$, together with the projections p_1 and p_2, is the fibred product of Y and W over X. Since p_2 is obtained by gluing the $p_2^{(n)}$'s, which are totally split, by lemma 2.2.40 we have that p_2 is totally split. This ends the proof. □

Remark 2.2.44. (1) Retracing the proof of the proposition 2.2.43, we can see that we could have required g to be finite étale, instead of just finite and locally free. Indeed, we constructed g through the following steps:

(i) $[Y : X] = 0$: we chose $g := \mathrm{id}_X$, which is finite étale;

(ii) inductive step: we defined $g := f \circ g'$, where g' existed by the inductive hypothesis;

(iii) non-constant degree: we glued the morphisms g_n, which existed because $[Y_n : X_n]$ had finite rank.

Since in the first step we had a finite étale morphism, we could modify the inductive hypothesis requiring that g be finite étale. Then in the second step we would have that g' is finite étale and, since f is finite étale by assumption, the composition $g = f \circ g'$ would be finite étale by lemma 2.2.30. Then, in the third point, each g_n would be finite étale and, by lemma 2.2.20, g would also be finite étale.

(2) From remark 2.2.38(1), it is clear that in the case of totally split morphisms the degree has the same meaning as the degree of finite coverings of topological spaces: the degree at a point is the cardinality of its preimage. One could be tempted to use 2.2.43 to generalize this to arbitrary finite étale morphisms. Let X, Y, W, $f : Y \to X$ and $g : W \to X$ be as in the claim of proposition 2.2.43. By 2.2.28(2), we have that $[Y \times_X W : W] = [Y : X] \circ g$. Since g is surjective, knowing the degree of $p_2 : Y \times_X W \to W$ allows us to know the degree of $f : Y \to X$ at any point $x \in X$. Indeed, let x in X. Since g is surjective, there exists $w \in W$ such that $x = g(w)$. Then we have that
$$[Y : X](x) = [Y : X](g(w)) = [Y \times_X W : W](w) = |p_2^{-1}(\{w\})|$$

(the last equality follows from the fact that p_2 is totally split). However, it is not true in general that $|p_2^{-1}(\{w\})| = |f^{-1}(\{x\})|$ (this holds for topological spaces, see 2.2.29, but nor for schemes, because the underlying topological space of the fibred product of schemes does not coincide with the fibred product of the underlying topological spaces). So we cannot conclude that $[Y : X](x) = |f^{-1}(\{x\})|$. Indeed, this is false in general.
As an example, let $X = \mathrm{Spec}(\mathbb{Q})$, $Y = \mathrm{Spec}(\mathbb{Q}(\sqrt{2}))$ and $f : Y \to X$ the morphism of schemes induced by the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2})$. We know that $\mathbb{Q}(\sqrt{2})$ is free of rank 2 over $\mathbb{Q}$, with basis $(1, \sqrt{2})$. Let $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$ be defined as in lemma 2.1.3(2). For any $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ $(a, b \in \mathbb{Q})$ we have that $m_{a+b\sqrt{2}}(1) = (a+b\sqrt{2})\cdot 1 = a+b\sqrt{2}$ and $m_{a+b\sqrt{2}}(\sqrt{2}) = (a+b\sqrt{2})\cdot\sqrt{2} = 2b + a\sqrt{2}$, so $\mathrm{Tr}(a + b\sqrt{2}) = a + a = 2a$. Then, for any $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ $(a, b \in \mathbb{Q})$, we have that

$$\varphi(a + b\sqrt{2})(1) = \mathrm{Tr}((a + b\sqrt{2}) \cdot 1) = \mathrm{Tr}(a + b\sqrt{2}) = 2a$$

and

$$\varphi(a + b\sqrt{2})(\sqrt{2}) = \mathrm{Tr}((a + b\sqrt{2}) \cdot \sqrt{2}) = \mathrm{Tr}(2b + a\sqrt{2}) = 2(2b) = 4b\,.$$

If $a+b\sqrt{2} \in \mathrm{Ker}(\varphi)$, i.e. $\varphi(a+b\sqrt{2}) = 0$, then we have that $0 = \varphi(a+b\sqrt{2})(1) = 2a$ and $0 = \varphi(a + b\sqrt{2})(\sqrt{2}) = 4b$, which implies that $a = 0$ and $b = 0$. So $a + b\sqrt{2} = 0$, which proves that $\mathrm{Ker}(\varphi) = 0$, i.e. φ is injective. Let now $\alpha \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$. Define $a := \frac{1}{2}\alpha(1) \in \mathbb{Q}$ and $b := \frac{1}{4}\alpha(\sqrt{2}) \in \mathbb{Q}$ and consider $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Then $\varphi(a + b\sqrt{2})(1) = 2a = 2 \cdot \frac{1}{2}\alpha(1) = \alpha(1)$ and $\varphi(a + b\sqrt{2})(\sqrt{2}) = 4b = 4 \cdot \frac{1}{4}\alpha(\sqrt{2}) = \alpha(\sqrt{2})$. Since $(1, \sqrt{2})$ generates $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, it follows that $\varphi(a + b\sqrt{2}) = \alpha$. Then φ is surjective. So φ is an isomorphism and this shows that $\mathbb{Q}(\sqrt{2})$ is a free separable $\mathbb{Q}$-algebra (one could actually show a more general result: if $k \subseteq K$ is any finite separable field extension, then K is a free separable k-algebra). Then f is finite étale. We have that $[Y : X] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = 2$. Moreover, $\mathrm{sp}(X) = \mathrm{sp}(\mathrm{Spec}(\mathbb{Q})) = \{0\}$ and $\mathrm{sp}(Y) = \mathrm{sp}(\mathrm{Spec}(\mathbb{Q}(\sqrt{2}))) = \{0\}$. So $|f^{-1}(\{0\})| = |\{0\}| = 1 \neq 2 = [Y : X](0)$. This shows that the degree of a finite étale morphism does not have the exact same meaning as the degree of a finite covering of a topological space, although they share some properties.

(3) In order to gain a better understanding of the meaning of proposition 2.2.43, we briefly introduce the notion of a *Grothendieck topology* (for more on this topic, see [6]). Given a category **C**, a Grothendieck topology on **C** is the assignment to each object U of **C** of a collection of families of morphisms $\{\varphi_i : U_i \to U\}_{i\in I}$ in **C** (called the *coverings* of U), such that:

(i) if $\varphi : V \to U$ is an isomorphism in **C**, then $\{\varphi : V \to U\}$ is a covering of U;

(ii) if $\{\varphi_i : U_i \to U\}_{i\in I}$ is a covering of U and $f : V \to U$ is any morphism in **C**, then for any $i \in I$ the fibred product $U_i \times_U V$ (with projections $p_1^{(i)} : U_i \times_U V \to U_i$ and $p_2^{(i)} : U_i \times_U V \to V$) exists and the family $\{p_2^{(i)} : U_i \times_U V \to V\}$ is a covering of V;

(iii) if $\{\varphi_i : U_i \to U\}_{i\in I}$ is a covering of U and for any $i \in I$ we have a covering $\{\psi_{ij} : V_{ij} \to U_i\}_{j\in J_i}$ of U_i, then $\{\varphi_i \circ \psi_{ij} : V_{ij} \to U\}_{i\in I, j\in J_i}$ is a covering of U.

This is a generalization of usual topological spaces in the following way: if X is a topological space, then we can consider the category $\mathbf{Op}_X$ whose objects are the open subsets of X and whose morphisms are the inclusions between them (notice that in this category the fibred product of two objects over a third one always exists and is given by the intersection of the two object, independently from the third one) and we can associate to any object U of $\mathbf{Op}_X$ the collection of families of the form $\{U_i \hookrightarrow U\}_{i\in I}$, where each U_i is an object of $\mathbf{Op}_X$ (i.e. an open subset of X) and $U = \bigcup_{i\in I} U_i$ (it is immediate to check that all the requirements are satisfied). If $\mathbf{C}$ is a category with a Grothendieck topology on it and P is a property enjoyed by some of the morphisms of $\mathbf{C}$, we say that a morphism $f : Y \to X$ in $\mathbf{C}$ enjoys P *locally* with respect to the given topology if there exists a covering $\{U_i \to X\}_{i\in I}$ of X such that the projection $p_1^{(i)} : U_i \times_X Y \to U_i$ enjoys P for every $i \in I$ (notice that the fibered product $U_i \times_X Y$ exists by (ii)).
The category we are interested in is the category $\mathbf{Sch}$ of schemes (or, more generally, the category $\mathbf{Sch}_S$ of schemes over a fixed scheme S; notice that $\mathbf{Sch} = \mathbf{Sch}_{\mathrm{Spec}(\mathbb{Z})}$). There are several Grothendieck topologies that can be defined on this category. In our case, we can consider as coverings of a schemes X the families of the form $\{g : W \to X\}$ with g surjective, finite and locally free. If $g : W \to X$ is an isomorphism, then it is in particular surjective. Moreover, it is totally split (example 2.2.36) and so finite étale (lemma 2.2.37), which implies finite and locally free (remark 2.2.4). So $\{g : W \to X\}$ is a covering of X. If $\{g : W \to X\}$ is a covering of X and $f : Y \to X$ is any morphism of schmes, then g is surjective, finite and locally free and by lemma 2.2.28(1),(3) we have that $p_2 : W \times_X Y \to Y$ is also surjective, finite and locally free (the fibred product always exists in the category of schemes) and so $\{p_2 : W \times_X Y \to Y\}$ is a covering of Y. Finally, if $\{g : W \to X\}$ is a covering of X and $\{h : V \to W\}$ is a covering of W, then g and h are both surjective, finite and locally free and so, by lemma 2.2.30, $g \circ h$ is finite and locally free. Moreover, the composition of surjective maps is surjective, so $g \circ h$ is surjective. Then $\{g \circ h : V \to X\}$ is a covering of X. This shows that we defined indeed a Grothendieck topology. Now 2.2.43 says that an affine morphism of schemes $f : Y \to X$ is finite étale if and only if there exists a covering $\{W \to X\}$ of X such that $p_2 : Y \times_X W \to W$ is totally split. This means (recalling that the fibred product is symmetric) that f is finite étale if and only if it is locally totally split. Recalling that totally split morphisms (of constant degree, but this is automatically true if X is connected) correspond to trivial finite coverings of topological spaces (remark 2.2.38(2)) and that finite coverings of topological spaces are defined as continuous maps which are locally trivial finite coverings, we see that we have a big similarity between finite étale coverings of a scheme and finite coverings of a topological space.
The Grothendieck topology we have just introduced fitted very well with our

purpose, but it is not one of the usual Grothendieck topologies that algebraic geometers work with. In fact, it is not even comparable with some of these topologies. A more common Grothendieck topology which is also relevant to our situation is the *fppf topology* (the acronym stands for "fidèlement plat et de présentation finie", i.e. "faithfully flat and of finite presentation"), in which a covering of a scheme X is given by a family $\{\varphi_i : U_i \to X\}_{i\in I}$ such that each φ_i is *flat* and *locally of finite presentation* (for the definitions, see [5], 24.2.6 and 7.3.17, respectively) and $X = \bigcup_{i\in I} \varphi_i(U_i)$ (the last condition can be expressed saying that the family $\{\varphi_i\}_{i\in I}$ is *jointly surjective*). It can be proved that a morphism is finite and locally free if and only if it is finite, flat and locally of finite presentation (see [1], 6.6, noticing that, according to the definition given in [1], 6.4, a morphism is *finitely presented* if and only if it is finite and locally of finite presentation). In particular, any finite and locally free morphism is flat and locally of finite presentation. So, if $g : W \to X$ is surjective, finite and locally free, we have that $\{g : W \to X\}$ is a covering of X in the fppf topology. Then, as above, we can use 2.2.43 to conclude that any finite étale morphism is locally totally split in the fppf topology.

(4) We will use proposition 2.2.43 in order to reduce proofs about finite étale morphisms to the case of totally split morphisms, which will often be much easier to deal with. As an example of this use, we give an alternative proof of lemma 2.2.30 in the case of finite étale morphisms (you can compare this approach to what we did in remark 2.2.31). Notice that in the proof of 2.2.43 we used 2.2.30 only in the case of finite and locally free morphisms, so we could have postponed until now the proof of that lemma in the case of finite étale morphisms, sparing us the algebraic work that underlay the proof we gave (corollary 2.1.69 and the preceding results).
Let X, Y anz Z be schemes and let $f_1 : Y \to X$, $f_2 : Z \to Y$ be two finite étale morphisms. First of all, assume that f_1 is totally split. Then we can write $X = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n$ for some schemes $X_0, X_1, \dots$ such that, for any $n \in \mathbb{Z}$, $n \geq 0$, there exists an isomorphism of schemes $\varphi_n : f_1^{-1}(X_n) \to \coprod_{i=1}^n X_n$ such that $p_n \circ \varphi_n = f_1$, where $p_n : \coprod_{i=1}^n X_n$ is obtained by gluing the identity morphisms $\mathrm{id}_{X_n} : X_n \to X_n$. For any $n \in \mathbb{Z}$, $n \geq 0$, define $Z_n := (f_1 \circ f_2)^{-1}(X_n)$. Then $Z = (f_1 \circ f_2)^{-1}(X) = (f_1 \circ f_2)^{-1}\left(\coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} X_n\right) = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} (f_1 \circ f_2)^{-1}(X_n) = \coprod_{\substack{n\in\mathbb{Z}\\ n\geq 0}} Z_n$. By lemma 2.2.20, in order to prove that $f_1 \circ f_2$ is finite étale, it is enough to prove that the restriction $(f_1 \circ f_2)_{|Z_n} : Z_n = (f_1 \circ f_2)^{-1}(X_n) \to X_n$ is finite étale for every $n \in \mathbb{Z}$, $n \geq 0$. Fix such an n. We have that $Z_n = (f_1 \circ f_2)^{-1}(X_n) = f_2^{-1}(f_1^{-1}(X_n))$. So $f_2(Z_n) \subseteq f_1^{-1}(X_n)$. Then we can consider the morphism $\varphi_n \circ f_2 : Z_n \to \coprod_{i=1}^n X_n$. We claim that this morphism is finite étale. Let $U = \mathrm{Spec}(A)$ be an open affine subset of $\coprod_{i=1}^n X_n$. Since $\varphi_n : f_1^{-1}(X_n) \to \coprod_{i=1}^n X_n$ is an isomorphism, we have that $\varphi_n^{-1}(U) \cong U = \mathrm{Spec}(A)$. Then, since f_2 is finite étale, by lemma 2.2.10(4) we have that $f_2^{-1}(\varphi_n^{-1}(U)) = (\varphi_n \circ f_2)^{-1}(U)$ is affine and equal to $\mathrm{Spec}(B)$, where B is a projective separable A-algebra. Since this holds for any open affine subset $U = \mathrm{Spec}(A)$ of $\coprod_{i=1}^n X_n$,

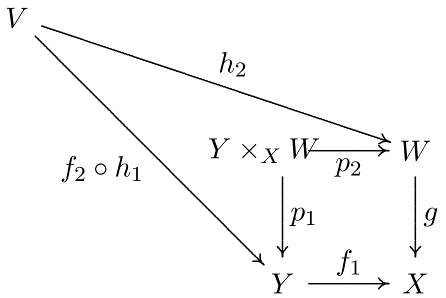
by lemma 2.2.10(4) we have that $\varphi_n \circ f_2 : Z_n \to \coprod_{i=1}^n X_n$ is finite étale. For any $i = 1, \dots, n$, let Z_{ni} be the preimage of the i-th copy of X_n under $\varphi_n \circ f_2$. Then $Z_n = (\varphi_n \circ f_2)^{-1} \left(\coprod_{i=1}^n X_n\right) = \coprod_{i=1}^n (\varphi_n \circ f_2)^{-1}(X_n) = \coprod_{i=1}^n Z_{ni}$. Fix $i \in \{1, \dots, n\}$. Then $(\varphi_n \circ f_2)_{|Z_{ni}} : Z_{ni} \to X_n$ is finite étale, by corollary 2.2.24. Notice that

$$(\varphi_n \circ f_2)_{|Z_{ni}} = \mathrm{id}_{X_n} \circ (\varphi_n \circ f_2)_{|Z_{ni}} = (p_n)_{|X_n} \circ \varphi_n \circ (f_2)_{|Z_{ni}} = \\ = p_n \circ \varphi_n \circ (f_2)_{|Z_{ni}} = f_1 \circ (f_2)_{|Z_{ni}} = (f_1 \circ f_2)_{|Z_{ni}} .$$

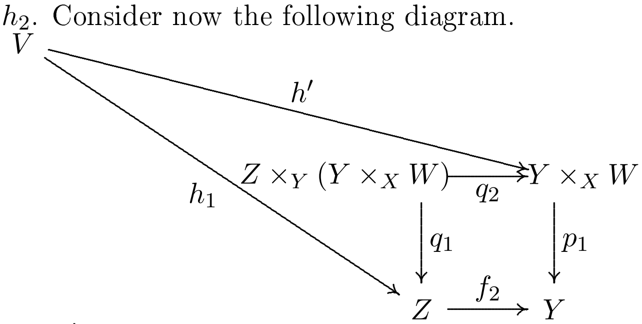
Then $(f_1 \circ f_2)_{|Z_{ni}} : Z_{ni} \to X_n$ is finite étale. Since this holds for any $i = 1, \dots, n$, by lemma 2.2.18(3) we have that $f_1 \circ f_2 : \coprod_{i=1}^n Z_{ni} = Z_n \to X_n$ is finite étale. Let now f_1 be an arbitrary finite étale morphism. By proposition 2.2.43 there exist a scheme W and a surjective, finite and locally free morphism $g : W \to X$ such that the projection $p_2 : Y \times_X W \to W$ is totally split. Let $p_1 : Y \times_X W \to Y$ be the first projection and consider the fibred product $Z \times_Y (Y \times_X W)$, with projections $q_1 : Z \times_Y (Y \times_X W) \to Z$ and $q_2 : Z \times_Y (Y \times_X W) \to Y \times_X W$. Since f_2 is finite étale, by lemma 2.2.28(4) we have that q_2 is finite étale. Then, since $p_2 : Y \times_X W \to W$ is totally split, by what we proved above $p_2 \circ q_2 : Z \times_Y (Y \times_X W) \to W$ is finite étale. By definition of fibred product, we have that $f_1 \circ p_1 = g \circ p_2$ and $f_2 \circ q_1 = p_1 \circ q_2$. Then

$$(f_1 \circ f_2) \circ q_1 = f_1 \circ p_1 \circ q_2 = g \circ (p_2 \circ q_2) .$$

Moreover, let V be a scheme with two morphisms of schemes $h_1 : V \to Z$ and $h_2 : V \to W$ such that $(f_1 \circ f_2) \circ h_1 = g \circ h_2$. Consider then the following diagram.



Since $f_1 \circ (f_2 \circ h_1) = g \circ h_2$, by the universal property of the fibred product there exists a unique morphism $h' : V \to Y \times_X W$ such that $p_1 \circ h' = f_2 \circ h_1$ and $p_2 \circ h' = h_2$. Consider now the following diagram.



Since $f_2 \circ h_1 = p_1 \circ h'$, by the universal property of the fibred product there exists a unique morphism $h : V \to Z \times_Y (Y \times_X W)$ such that $q_1 \circ h = h_1$ and $q_2 \circ h = h'$. Then we have that $(p_2 \circ q_2) \circ h = p_2 \circ h' = h_2$. Let $\widetilde{h} : V \to Z \times_Y (Y \times_X W)$ be another morphism of schemes such that $q_1 \circ \widetilde{h} = h_1$ and $(p_2 \circ q_2) \circ \widetilde{h} = h_2$. Then $p_1 \circ (q_2 \circ \widetilde{h}) = f_2 \circ q_1 \circ \widetilde{h} = f_2 \circ h_1$ and $p_2 \circ (q_2 \circ \widetilde{h}) = h_1$. By uniqueness of h', this implies that $q_2 \circ \widetilde{h} = h'$. Since we had also $q_1 \circ \widetilde{h} = h_1$, we must have $\widetilde{h} = h$. This proves that $Z \times_Y (Y \times_X W)$, together with the morphisms $q_1 : Z \times_Y (Y \times_X W) \to Z$ and $p_2 \circ q_2 : Z \times_Y (Y \times_X W) \to W$, is the fibred product of Z and W over X. Since $p_2 \circ q_2$ is finite étale and g is surjective, finite and locally free, by lemma 2.2.34, we have that $f_1 \circ f_2$ is finite étale.

From now on, we will adopt the following notation: if X is a scheme and E is a finite set, we will write $X \times E := \coprod_{e \in E} X$ (disjoint union of schemes). This notation is motivated by what we did in remark 2.2.38(2), where we saw that, if X and E are topological spaces with E discrete, then $X \times E = \coprod_{e \in E} X \times \{e\}$ and each $X \times \{e\}$ is homeomorphic to X.

Lemma 2.2.45. *Let X be a scheme, D and E finite sets. Any map $\varphi : D \to E$ induces a morphism of schemes $X \times D \to X \times E$, which is finite étale (we will denote this morphism by $\mathrm{id}_X \times \varphi$, in analogy to what happens for topological spaces).*

Proof. Let $\varphi : D \to E$ be any map. For any $e \in E$, denote by $q_e : X \to \coprod_{e \in E} X = X \times E$ the e-th inclusion, which is a morphism of schemes. Then for any $d \in D$ we have a morphism of schemes $q_{\varphi(d)} : X \to X \times E$. Gluing these morphisms, we get a morphism $\coprod_{d \in D} X = X \times D \to X \times E$. From now on, we denote this morphism by $\mathrm{id}_X \times \varphi$.
In order to avoid confusion, denote the d-th copy of X in $X \times D = \coprod_{d \in D} X$ by X_d, for any $d \in D$, and the e-th copy of X in $X \times E = \coprod_{e \in E} X$ by X_e, for any $e \in E$. We have that $X \times D = (\mathrm{id}_X \times \varphi)^{-1}(X \times E) = (\mathrm{id}_X \times \varphi)^{-1}\left(\coprod_{e \in E} X_e\right) = \coprod_{e \in E} (\mathrm{id}_X \times \varphi)^{-1}(X_e)$. By lemma 2.2.20, in order to prove that $\mathrm{id}_X \times \varphi$ is finite étale, it is enough to prove that $(\mathrm{id}_X \times \varphi)_{|(\mathrm{id}_X \times \varphi)^{-1}(X_e)} : (\mathrm{id}_X \times \varphi)^{-1}(X_e) \to X_e$ is finite étale for every $e \in E$. Fix $e \in E$. By definition of $\mathrm{id}_X \times \varphi$, we have that $(\mathrm{id}_X \times \varphi)^{-1}(X_e) = \coprod_{d \in D} q^{-1}_{\varphi(d)}(X_e)$. Moreover, by definition of $q_{\varphi(d)}$, for every $d \in D$ we have that $q^{-1}_{\varphi(d)}(X_e)$ is empty if $\varphi(d) \neq e$ and equal to X_d if $\varphi(d) = e$. Then $(\mathrm{id}_X \times \varphi)^{-1}(X_e) = \coprod_{d \in \varphi^{-1}(\{e\})} X_d$. So the restriction $(\mathrm{id}_X \times \varphi)_{|(\mathrm{id}_X \times \varphi)^{-1}(X_e)} : (\mathrm{id}_X \times \varphi)^{-1}(X_e) = \coprod_{d \in \varphi^{-1}(\{e\})} X_d \to X_e$ is totally split (define $X_{en} := X$ and $\varphi_{en} := \mathrm{id}_{\coprod_{d \in \varphi^{-1}(\{e\})} X_d}$ if $n = |\varphi^{-1}(d)|$ and $X_{en} := \emptyset$ otherwise). Then this restriction is finite étale by lemma 2.2.37. □

We are now going to prove the analogue of the lemma 1.5 of the appendix: having saw that finite étale morphisms are "locally trivial", we want to show that also morphisms between them are "locally trivial". In order to do that, we need two algebraic lemmas.

Lemma 2.2.46. *For any ring A and any finite set E, define $A^E := \prod_{e \in E} A$ (with componentwise operations, which make it into a ring; then the ring homomorphism $\vartheta_E : A \to A^E$, $a \mapsto (a, \ldots, a)$ makes A^E into an A-algebra). Let A be a ring with no non-trivial idempotents (i.e., if $a \in A$ and $a^2 = a$, then $a = 0$ or $a = 1$) and let*

D, E be finite sets. Then any map $\varphi : D \to E$ induces an A-algebra homomorphism $\Phi : A^E \to A^D$ and all A-algebra homomorphisms $A^E \to A^D$ are of this form.

Proof. If $\varphi : D \to E$ is any map, we can define $\Phi : A^E \to A^D$, $(a_e)_{e\in E} \mapsto (a_{\varphi(d)})_{d\in D}$. For any $(a_e)_{e\in E}, (b_e)_{e\in E} \in A^E$, we have that

$$\Phi((a_e)_{e\in E} + (b_e)_{e\in E}) = \Phi((a_e + b_e)_{e\in E}) = (a_{\varphi(d)} + b_{\varphi(d)})_{d\in D} = \\ = (a_{\varphi(d)})_{d\in D} + (b_{\varphi(d)})_{d\in D} = \Phi((a_e)_{e\in E}) + \Phi((b_e)_{e\in E})$$

and

$$\Phi((a_e)_{e\in E} \cdot (b_e)_{e\in E}) = \Phi((a_e \cdot b_e)_{e\in E}) = (a_{\varphi(d)} \cdot b_{\varphi(d)})_{d\in D} = \\ = (a_{\varphi(d)})_{d\in D} \cdot (b_{\varphi(d)})_{d\in D} = \Phi((a_e)_{e\in E}) \cdot \Phi((b_e)_{e\in E}) \ .$$

Moreover, $\Phi(1_{A^E}) = \Phi((1)_{e\in E}) = (1)_{d\in D} = 1_{A^D}$. So Φ is a ring homomorphism. For any $a \in A$, we have that

$$\Phi(\vartheta_E(a)) = \Phi((a)_{e\in E}) = (a)_{d\in D} = \vartheta_D(a) \ .$$

Then $\Phi \circ \vartheta_E = \vartheta_D$, which means that Φ is an A-algebra homomorphism.
Let $f : A^E \to A^D$ be any A-algebra homomorphism. If $A = 0$, then $A^E = A^D = 0$ and so $f = 0$ is induced by any map $\varphi : D \to E$. Assume now that $A \neq 0$. For any $e \in E$, define $x_e := (\delta_{ee'})_{e'\in E} \in A^E$. Notice that $x_e^2 = x_e$, for every $e \in E$. Let $d \in D$ and define $p_d : A^D \to A$, $(a_{d'})_{d'\in D} \mapsto a_d$. It is immediate to check that p_d is an A-algebra homomorphism. Then $p_d \circ f : A^E \to A$ is an A-algebra homomorphism (because it is a composition of A-algebra homomorphisms) and, for every $e \in E$, we have that $(p_d \circ f)(x_e) = (p_d \circ f)(x_e^2) = (p_d \circ f)(x_e)^2$, which by assumption implies that $(p_d \circ f)(x_e) \in \{0, 1\}$. Moreover, $1_{A^E} = (1)_{e\in E} = (\sum_{e\in E} \delta_{ee'})_{e'\in E} = \sum_{e\in E}(\delta_{ee'})_{e'\in E} = \sum_{e\in E} x_e$ and so $1 = (p_d \circ f)(1_{A^E}) = (p_d \circ f)\left(\sum_{e\in E} x_e\right) = \sum_{e\in E}(p_d \circ f)(x_e)$. This implies that there exists at least one $e \in E$ such that $(p_d \circ f)(x_e) \neq 0$, and so $(p_d \circ f)(x_e) = 1$. We claim that such an e is unique. Let $e_1, e_2 \in E$ be such that $(p_d \circ f)(x_{e_1}) = 1 = (p_d \circ f)(x_{e_2})$ and assume by contradiction that $e_1 \neq e_2$. Then $x_{e_1} \cdot x_{e_2} = 0$ and, since $p_d \circ f$ is a ring homomorphism,

$$0 = (p_d \circ f)(0) = (p_d \circ f)(x_{e_1} \cdot x_{e_2}) = (p_d \circ f)(x_{e_1}) \cdot (p_d \circ f)(x_{e_2}) = 1 \cdot 1 = 1 \ .$$

This is a contradiction. Then there exists a unique $e \in E$ such that $(p_d \circ f)(x_e) = 1$. Let $\varphi(d)$ be this e. Then we have a map $\varphi : D \to E$ such that $(p_d \circ f)(x_e) = \delta_{e\varphi(d)}$ for any $d \in D$, $e \in E$. Let $\Phi : A^E \to A^D$ be the morphism induced by φ, as above. We claim that $f = \Phi$. Let $x = (a_{e'})_{e'\in E} \in A^E$. We have that $x = (a_{e'})_{e'\in E} = (\sum_{e\in E} a_e\delta_{ee'})_{e'\in E} = \sum_{e\in E}(a_e\delta_{ee'})_{e'\in E} = \sum_{e\in E} a_e x_e$. Then, for any $d \in D$,

$$(p_d \circ f)(x) = (p_d \circ f)\left(\sum_{e\in E} a_e x_e\right) = \sum_{e\in E} a_e (p_d \circ f)(x_e) = \sum_{e\in E} a_e \delta_{e\varphi(d)} = a_{\varphi(d)} \ ,$$

because $p_d \circ f$ is an A-algebra homomorphism. It follows that

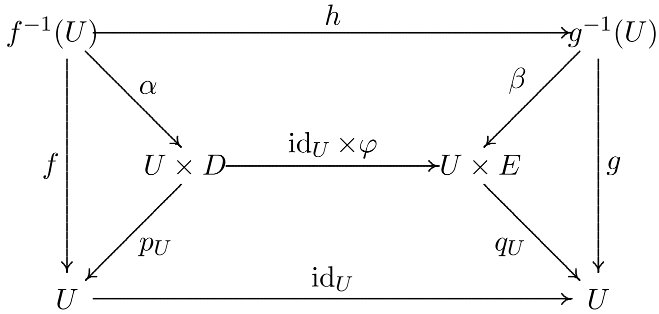
$$f(x) = ((p_d \circ f)(x))_{d\in D} = (a_{\varphi(d)})_{d\in D} = \Phi((a'_e)_{e'\in E}) = \Phi(x) \ .$$

This proves the claim. □

Lemma 2.2.47. *Let A be a local ring. Then A has no non-trivial idempotents.*

Proof. Let $\mathfrak{m} = A \backslash A^{\times}$ be the unique maximal ideal of A and let $a \in A$ be such that $a^2 = a$. This means that $a(a-1) = a^2 - a = 0 \in \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, it is in particular prime. Then we have that either $a \in \mathfrak{m}$ or $a - 1 \in \mathfrak{m}$. Assume that $a \in \mathfrak{m}$. If we had also $a - 1 \in \mathfrak{m}$, we would have that $1 = a - (a-1) \in \mathfrak{m}$, because $\mathfrak{m}$ is an ideal, but this is a contradiction, because $\mathfrak{m}$ is a proper ideal. So $a - 1 \in A \backslash \mathfrak{m} = A^{\times}$. It follows that $a = a(a-1)(a-1)^{-1} = 0 \cdot (a-1)^{-1} = 0$. In the same way, one shows that if $a - 1 \in \mathfrak{m}$ then $a - 1 = 0$, i.e. $a = 1$. □

Lemma 2.2.48. *Let X, Y, Z be schemes, $f : Y \to X$ and $g : Z \to X$ totally split morphisms and $h : Y \to Z$ a morphism of schemes such that $f = g \circ h$. For any $x \in X$, there exists an open affine neighbourhood U of x in X such that f, g and h are "trivial above U", i.e. such that there exist finite sets D and E, isomorphisms of schemes $\alpha : f^{-1}(U) \to U \times D$ and $\beta : g^{-1}(U) \to U \times E$ and a map $\varphi : D \to E$ such that the following diagram is commutative, where $p_U : U \times D = \coprod_{d \in D} U \to U$ and $q_U : U \times E = \coprod_{e \in E} \to U$ are the morphisms obtained by gluing the identity morphisms $\mathrm{id}_U : U \to U$.*



Proof. Since f is totally split, there exist some schemes $X_0, X_1, \ldots$ such that $X = \coprod_{\substack{n \in \mathbb{Z} \\ n \geq 0}} X_n$ and, for any $n \in \mathbb{Z}$, $n \geq 0$, there exists an isomorphism of schemes $\alpha_n : f^{-1}(X_n) \to \coprod_{i=1}^{n} X_n$ such that $p_n \circ \alpha_n = f$, where $p_n : \coprod_{i=1}^{n} X_n \to X_n$ is obtained by gluing the identity morphisms $\mathrm{id}_{X_n} : X_n \to X_n$. Analogously, since g is totally split, we can write $X = \coprod_{\substack{m \in \mathbb{Z} \\ m \geq 0}} X'_m$ for some schemes $X'_0, X'_1, \ldots$ such that, for any $m \in \mathbb{Z}$, $m \geq 0$, there exists an isomorphism of schemes $\beta_m : f^{-1}(X'_m) \to \coprod_{j=1}^{m} X'_m$ such that $q_m \circ \beta_m = g$, where $q_m : \coprod_{j=1}^{m} X'_m \to X'_m$ is obtained by gluing the identity morphisms $\mathrm{id}_{X'_m} : X'_m \to X'_m$. Since $x \in X = \coprod_{\substack{n \in \mathbb{Z} \\ n \geq 0}} X_n = \coprod_{\substack{m \in \mathbb{Z} \\ m \geq 0}} X'_m$, there exist $n, m \in \mathbb{Z}$, $n, m \geq 0$ such that $x \in X_n$ and $x \in X'_m$. Then $x \in X_n \cap X'_m$. Define $D := \{1, \ldots, n\}$ and $E := \{1, \ldots, m\}$. We have that X_n and X'_m are both open in X by definition of disjoint union, so $X_n \cap X'_m$ is an open subscheme of X. By definition of scheme, there exists an open affine subset $V = \mathrm{Spec}(A)$ of $X_n \cap X'_m$ such that $x \in V$. Since $V \subseteq X_n$ and $p_n \circ \alpha_n = f$, we have that $f^{-1}(V) = (p_n \circ \alpha_n)^{-1}(V) = \alpha_n^{-1}(p_n^{-1}(V)) = \alpha_n^{-1}(V \times D)$. Then, restricting α_n to $f^{-1}(V)$, we get an isomorphism of schemes $\alpha_n : f^{-1}(V) = \alpha_n^{-1}(V \times D) \to V \times D$. Analogously, since $V \subseteq X'_m$ and $q_m \circ \beta_m = g$, we have that $g^{-1}(V) = (q_m \circ \beta_m)^{-1}(V) = \beta_m^{-1}(q_m^{-1}(V)) = \beta_m^{-1}(V \times E)$. Then, restricting β_m to $g^{-1}(V)$, we get an isomorphism of schemes $\beta_m : g^{-1}(V) = \beta_m^{-1}(V \times E) \to V \times E$. Since $f = g \circ h$, we have that $f^{-1}(V) = (g \circ h)^{-1}(V) = h^{-1}(g^{-1}(V))$, so

$h(f^{-1}(V)) \subseteq g^{-1}(V)$. Then we can consider the morphism of schemes $\beta_m \circ h \circ \alpha_n^{-1} : V \times D \to V \times E$. We have that $V \times D = \coprod_{i=1}^n V = \coprod_{i=1}^n \operatorname{Spec}(A) = \operatorname{Spec}(\prod_{i=1}^n A) = \operatorname{Spec}(A^D)$ and $V \times E = \coprod_{j=1}^m V = \coprod_{j=1}^m \operatorname{Spec}(A) = \operatorname{Spec}(\prod_{j=1}^m A) = \operatorname{Spec}(A^E)$ (this can be checked as in the proof of lemma 2.2.18). Then $\beta_m \circ h \circ \alpha_n^{-1} : V \times D = \operatorname{Spec}(A^D) \to V \times E = \operatorname{Spec}(A^E)$ corresponds to a ring homomorphism $\psi : A^E \to A^D$. The restriction $p_n : p_n^{-1}(V) = V \times D = \operatorname{Spec}(A^D) \to V = \operatorname{Spec}(A)$ corresponds to the ring homomorphism $\vartheta_D : A \to A^D$, $a \mapsto (a)_{d \in D}$. Analogously, the restriction $q_m : q_m^{-1}(V) = V \times E = \operatorname{Spec}(A^E) \to V = \operatorname{Spec}(A)$ corresponds to the ring homomorphism $\vartheta_E : A \to A^E$, $a \mapsto (a)_{e \in E}$. Recalling that $p_n \circ \alpha_n = f$, $q_m \circ \beta_m = g$ and $g \circ h = f$, we get that

$$q_m \circ (\beta_m \circ h \circ \alpha_n^{-1}) = g \circ h \circ \alpha_n^{-1} = f \circ \alpha_n^{-1} = p_n .$$

In terms of ring homomorphisms, this means that $\psi \circ \vartheta_E = \vartheta_D$, i.e. $\psi : A^E \to A^D$ is an A-algebra homomorphism. Since $x \in V = \operatorname{Spec}(A)$, we can consider the localization A_x, which is a local ring, and the localized map $\psi_x : (A^E)_x \to (A^D)_x$, which is A_x-linear. Since the localization commutes with direct sums (see lemma 2.1.19, recalling that localization at x corresponds to tensor product with A_x) and a finite product of modules coincides with their direct sum, we have that $(A^E)_x = \left(\bigoplus_{j=1}^m A\right)_x \cong \bigoplus_{j=1}^m A_x = (A_x)^E$ and $(A^D)_x = (\bigoplus_{i=1}^n A)_x \cong \bigoplus_{i=1}^n A_x = (A_x)^D$ as A_x-modules. Let $\psi_E : (A^E)_x \to (A_x)^E$ and $\psi_D : (A^D)_x \to (A_x)^D$ be the corresponding isomorphims, analogously to lemma 2.1.19. It is immediate to check that ψ_x, ψ_E and ψ_D are ring homomorphisms, if we consider the obvious ring structures, so they are homomorphisms of A_x-algebras. Then the composition $\psi_D \circ \psi_x \circ \psi_E^{-1} : (A_x)^E \to (A_x)^D$ is also a homomorphism of A_x-algebras. By lemma 2.2.47, we have that A_x has no non-trivial idempotents. Then, by lemma 2.2.46, there exists a map $\varphi : D \to E$ such that $\psi_D \circ \psi_x \circ \psi_E^{-1}$ is induced by φ. This means that $(\psi_D \circ \psi_x \circ \psi_E)^{-1}((\alpha_1, \dots, \alpha_m)) = (\alpha_{\varphi(1)}, \dots, \alpha_{\varphi(n)})$ for any $(\alpha_1, \dots, \alpha_m) \in (A_x)^E$. Let $\Phi : A^E \to A^D$ be the A-algebra homomorphism induced by φ. Localizing it at x, we get an A_x-algebra homomorphism $\Phi_x : (A^E)_x \to (A^D)_x$ (analogously to ψ_x, this is A_x-linear by definition of localization and it can be easily checked that it is a ring homomorphism). For any $\left(\frac{a_1}{s_1}, \dots, \frac{a_m}{s_m}\right) \in (A_x)^E$ ($a_1, \dots, a_m \in A$, $s_1, \dots, s_m \in A \backslash x$), we have that

$$(\psi_D \circ \Phi_x \circ \psi_E^{-1}) \left(\left(\frac{a_1}{s_1}, \dots, \frac{a_m}{s_m} \right) \right) = \psi_D \left(\Phi_x \left(\sum_{j=1}^m \frac{(a_j \delta_{jj'})_{j'=1,\dots,m}}{s_j} \right) \right) =$$

$$= \psi_D \left(\sum_{j=1}^m \frac{\Phi((a_j \delta_{jj'})_{j'=1,\dots,m})}{s_j} \right) = \sum_{j=1}^m \psi_D \left(\frac{(a_j \delta_{j\varphi(i)})_{i=1,\dots,n}}{s_j} \right) =$$

$$= \sum_{j=1}^m \left(\frac{a_j \delta_{j\varphi(i)}}{s_j} \right)_{i=1,\dots,n} = \left(\sum_{j=1}^m \frac{a_j \delta_{j\varphi(i)}}{s_j} \right)_{i=1,\dots,n} =$$

$$= \left(\frac{a_{\varphi(i)}}{s_{\varphi(i)}} \right)_{i=1,\dots,n} = (\psi_D \circ \psi_x \circ \psi_E^{-1}) \left(\left(\frac{a_1}{s_1}, \dots, \frac{a_m}{s_m} \right) \right) .$$

So $\psi_D \circ \Phi_x \circ \psi_E^{-1} = \psi_D \circ \psi_x \circ \psi_E^{-1}$, which implies that $\Phi_x = \psi_x$. Notice that A^E is finitely presented as an A-module, because it is a free A-module of finite rank (you can consider the exact sequence $0 \to A^E = A^m \xrightarrow{\mathrm{id}_{A^E}} A^E = A^m \to 0$). Then, by lemma 2.1.27, we have an isomorphism of A_x-modules $\mathrm{Hom}_A(A^E, A^D)_x \to \mathrm{Hom}_{A_x}((A^E)_x, (A^D)_x)$. We denote this isomorphism by χ. Then $\psi_x = \chi\left(\frac{\psi}{1}\right)$ and $\Phi_x = \chi\left(\frac{\Phi}{1}\right)$. Then $\chi\left(\frac{\psi}{1}\right) = \psi_x = \Phi_x = \chi\left(\frac{\Phi}{1}\right)$. Since χ is bijective, it follows that $\frac{\psi}{1} = \frac{\Phi}{1}$ in $\mathrm{Hom}_A(A^E, A^D)_x$. This means that there exists $u \in A \backslash x$ such that $u(\psi \cdot 1 - \Phi \cdot 1) = 0$, i.e. $u\psi = u\Phi$. Then we have also $\frac{\psi}{1} = \frac{\Phi}{1}$ in $\mathrm{Hom}_A(A^E, A^D)_u$.
Define $U := V_u = \mathrm{Spec}(A_u) \subseteq V$. Since $u \notin x$, we have that $x \in V_u = U$. So U is an open affine neighbourhood of x. Since $U \subseteq V \subseteq X_n$ and $p_n \circ \alpha_n = f$, we have that $f^{-1}(U) = \alpha_n^{-1}(U \times D)$ (see above) and, restricting α_n to $f^{-1}(U)$, we get an isomorphism of schemes $\alpha := \alpha_n : f^{-1}(U) = \alpha_n^{-1}(U \times D) \to U \times D$. From the definition of p_n, it is clear that its restriction $p_n : p_n^{-1}(U) = U \times D \to U$ coincides with p_U (defined as in the statement). Since $p_n \circ \alpha_n = f$, we have that $p_U \circ \alpha = f$. Analogously, since $U \subseteq V \subseteq X'_m$ and $q_m \circ \beta_m = g$, we have that $g^{-1}(U) = \beta_m^{-1}(U \times E)$ (see above). Then, restricting β_m to $g^{-1}(U)$, we get an isomorphism of schemes $\beta := \beta_m : g^{-1}(U) = \beta_m^{-1}(U \times E) \to U \times E$. From the definition of q_m, it is clear that its restriction $q_m : q_m^{-1}(U) = U \times E \to U$ coincides with q_U (defined as in the statement). Since $q_m \circ \beta_m = g$, we have that $q_U \circ \beta = g$. From the definitions of p_U, q_U and $\mathrm{id}_U \times \varphi$ (see lemma 2.2.45), we have that $q_U \circ (\mathrm{id}_U \times \varphi) = p_U = \mathrm{id}_U \circ p_U$ (for any $d \in D$, the restriction of $q_U \circ (\mathrm{id}_U \times \varphi)$ to the d-th copy of U in $U \times D = \coprod_{i=1}^n U$ is $p_U \circ q_{\varphi(d)} : U \to U$, where $q_{\varphi(d)} : U \to U \times E$ is as in the proof of 2.2.45, and this composition is equal to id_U by definition of p_U). It remains to prove the commutativity of the upper part of the diagram.
Since $f = g \circ h$, we have that $f^{-1}(U) = (g \circ h)^{-1}(U) = h^{-1}(g^{-1}(U))$. So $h(f^{-1}(U)) \subseteq g^{-1}(U)$. We have to prove that $\beta \circ h = (\mathrm{id}_U \times \varphi) \circ \alpha$. Consider $\beta \circ h \circ \alpha^{-1} : U \times D \to U \times E$. From the definitions of α and β, it is clear that $\beta \circ h \circ \alpha^{-1}$ is the restriction of $\beta_m \circ h \circ \alpha_n^{-1}$. We have that $U \times D = \mathrm{Spec}(A_u) \times D = \mathrm{Spec}((A_u)^D)$ and $U \times E = \mathrm{Spec}((A_u)^E)$ (this can be checked as we did above with V instead of U). Then

$$\beta \circ h \circ \alpha^{-1} : U \times D = \mathrm{Spec}((A_u)^D) \to U \times E = \mathrm{Spec}((A_u)^E)$$

corresponds to a ring homomorphism $\psi' : (A_u)^E \to (A_u)^D$. Since $\beta \circ h \circ \alpha^{-1}$ is the restriction of $\beta_m \circ h \circ \alpha_n^{-1}$ and the latter morphism corresponds to the ring homomorphism $\psi : A^E \to A^D$, we have that $\psi' = \psi_D \circ \psi_u \circ \psi_E^{-1}$. Since A^E is finitely presented, by lemma 2.1.27 we have an isomorphism of A_u-modules $\mathrm{Hom}_A(A^E, A^D)_u \to \mathrm{Hom}_{A_u}((A^E)_u, (A^D)_u)$. We denote this isomorphim by χ'. Then $\chi'\left(\frac{\psi}{1}\right) = \psi_u$ and $\chi'\left(\frac{\Phi}{1}\right) = \Phi_u$. We know that $\frac{\psi}{1} = \frac{\Phi}{1}$ in $\mathrm{Hom}_A(A^E, A^D)_u$, so $\psi_u = \Phi_u$. Then $\psi' = \psi_D \circ \Phi_u \circ \psi_E$. On the other hand, $\mathrm{id}_U \times \varphi : U \times D = \mathrm{Spec}((A_u)^D) \to U \times E = ((A_u)^E)$ corresponds to a ring homomorphism $\Phi' : (A_u)^E \to (A_u)^D$. By definition, $\mathrm{id}_U \times \varphi$ is obtained by gluing the morphisms $q_{\varphi(d)} : U \to U \times E = \coprod_{e \in E} U$ (see lemma 2.2.45). For any $d \in D$, we have that $q_{\varphi(d)} : U = \mathrm{Spec}(A_u) \to U \times E = \mathrm{Spec}((A_u)^E)$ corresponds to the ring homomorphism $\pi_{\varphi(d)} : (A_u)^E \to A_u$, $(\alpha_1, \ldots, \alpha_m) \mapsto \alpha_{\varphi(d)}$.

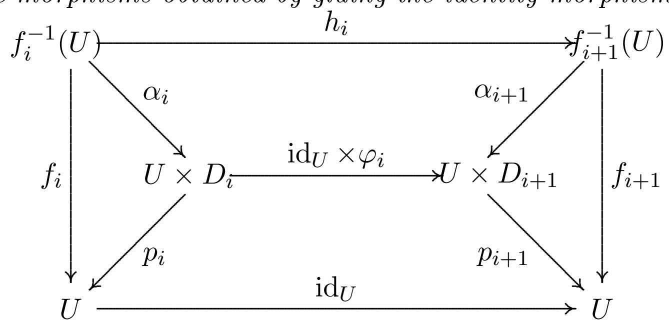
Then

$$\Phi'((\alpha_1, \dots, \alpha_m)) = (\alpha_{\varphi(1)}, \dots, \alpha_{\varphi(n)}) = (\psi_D \circ \Phi_u \circ \psi_E^{-1})((\alpha_1, \dots, \alpha_m))$$

(the last equality can be proved as we did above with Φ_x instead of Φ_u), for any $(\alpha_1, \dots, \alpha_m) \in A^E$. So $\Phi' = \psi_D \circ \Phi_u \circ \psi_E = \psi'$, which implies that $\mathrm{id}_U \times \varphi = \beta \circ h \circ \alpha^{-1}$. This ends the proof. □

As in the case of finite coverings of topological spaces (corollary 1.6 of the appendix), we can generalize the lemma we have just proved to a finite number of morphisms.

Corollary 2.2.49. *Let X, $Y_1, \dots, Y_n$ be schemes ($n \in \mathbb{N}$), $f_1 : Y_1 \to X, \dots, f_n : Y_n \to X$ totally split morphisms and $h_1 : Y_1 \to Y_2, \dots, h_{n-1} : Y_{n-1} \to Y_n$ morphisms of schemes such that $f_i = f_{i+1} \circ h_i$ for every $i = 1, \dots, n-1$. For any $x \in X$, there exists an open affine neighbourhood U of x in X such that $f_1, \dots, f_n$, $h_1, \dots, h_{n-1}$ are all trivial above U, in the same sense as in the lemma 2.2.48: there exist finite sets $D_1, \dots, D_n$, isomorphisms of schemes $\alpha_1 : f_1^{-1}(U) \to U \times D_1, \dots, \alpha_n : f_n^{-1}(U) \to U \times D_n$ and maps $\varphi_1 : D_1 \to D_2, \dots, \varphi_{n-1} : D_{n-1} \to D_n$ such that the following diagram is commutative for any $i = 1, \dots, n-1$, where $p_1 : U \times D_1 \to U, \dots, p_n : U \times D_n \to U$ are the morphisms obtained by gluing the identity morphisms $\mathrm{id}_U : U \to U$.*



Proof. By lemma 2.2.48, for any $i = 1, \dots, n-1$ there exists an open affine neighbourhood U_i of x in X such that f_i, f_{i+1} and h_i are trivial above U_i. Define $V := \bigcap_{i=1}^{n-1} U_i$. Then V is an open subscheme of X, because it is a finite intersection of open subschemes. Moreover, $x \in V$. Then, by definition of scheme, there exists an open affine subset U of V such that $x \in U$. So U is an open affine neighbourhood of x in X and, since $U \subseteq V \subseteq U_i$ for any $i = 1, \dots, n-1$, it is immediate to check that $f_1, \dots, f_n$, $h_1, \dots, h_{n-1}$ are all trivial above U. □

The first application of lemma 2.2.48 will be the proof that any morphism betweem finite étale coverings is itself finite étale.

Lemma 2.2.50. *Let X, Y and Z be schemes and let $g : Z \to X$, $h : Y \to Z$ be morphisms of schemes. If g and $g \circ h$ are both affine, then h is affine.*

Proof. Since $g \circ h : Z \to X$ is affine, there exists a cover of X by open affine subsets $(U_i)_{i \in I}$ such that $(g \circ h)^{-1}(U_i)$ is affine for every $i \in I$. Let $i \in I$. Since g is continuous and U_i is open in X, $g^{-1}(U_i)$ is open in Z. Moreover, since g is affine, by lemma 2.2.10(1) we have that $g^{-1}(U_i)$ is affine, because U_i is affine. Then $g^{-1}(U_i)$ is an open affine subset of Z. We have that

$$Z = g^{-1}(X) = g^{-1}\left(\bigcup_{i\in I} U_i\right) = \bigcup_{i\in I} g^{-1}(U_i) .$$

So $(g^{-1}(U_i))_{i\in I}$ is a cover of Z by open affine subsets. Since $h^{-1}(g^{-1}(U_i)) = (g \circ h)^{-1}(U_i)$ is affine for every $i \in I$, we have that h is affine. □

Lemma 2.2.51. *Let X, Y and Z be schemes and let $f_1 : Y \to X$, $f_2 : Z \to X$ be finite étale coverings of X. Let $h : Y \to Z$ be a morphism of coverings from f_1 to f_2 (i.e., h is a morphism of schemes such that $f_1 = f_2 \circ h$). Then h is finite étale.*

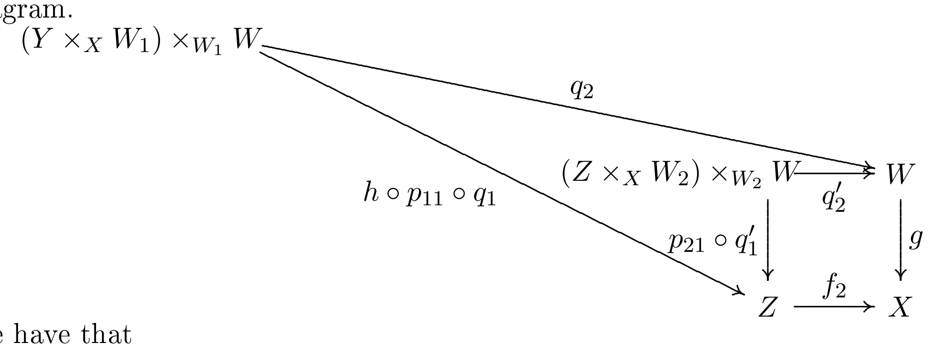
Proof. Assume firstly that f_1 and f_2 are totally split. For every $x \in X$, let U_x be an open affine neighbourhood of $x \in X$ such that f_1, f_2 and h are trivial above U_x, as in lemma 2.2.48. Then $X = \bigcup_{x\in X} U_x$ and so $Z = f_2^{-1}(X) = f_2^{-1}\left(\bigcup_{x\in X} U_x\right) = \bigcup_{x\in X} f_2^{-1}(U_x)$. Since f_2 is finite étale, it is in particular affine. Then, by lemma 2.2.10(3), we have that $f_2^{-1}(U_x)$ is affine for every $x \in X$. So $(f_2^{-1}(U_x))_{x\in X}$ is a cover of Z by open affine subsets. Fix $x \in X$ and let A_x be a ring such that $U_x = \mathrm{Spec}(A_x)$. By the choice of U_x, there exist finite sets D_x and E_x, isomorphisms of schemes $\alpha_x : f_1^{-1}(U_x) \to U_x \times D_x$ and $\beta_x : f_2^{-1}(U_x) \to U_x \times E_x$ and a map $\varphi_x : D_x \to E_x$ such that $h_{|_{f_1^{-1}(U_x)}} = \beta_x^{-1} \circ (\mathrm{id}_{U_x} \times \varphi_x) \circ \alpha_x$. By lemma 2.2.45, we have that $\mathrm{id}_{U_x} \times \varphi_x$ is finite étale. Moreover, α_x and β_x^{-1} are finite étale because they are isomorphisms (see 2.2.36, together with 2.2.37). Then the composition $h_{|_{f_1^{-1}(U_x)}} = \beta_x^{-1} \circ (\mathrm{id}_{U_x} \times \varphi_x) \circ \alpha_x$ is finite étale by lemma 2.2.30. Then, by lemma 2.2.10(4), we have that $\left(h_{|_{f_1^{-1}(U_x)}}\right)^{-1}(f_2^{-1}(U_x))$ is affine and equal to B_x, where B_x is a projective separable A_x-algebra. But

$$\left(h_{|_{f_1^{-1}(U_x)}}\right)^{-1}(f_2^{-1}(U_x)) = h^{-1}(f_2^{-1}(U_x)) \cap f_1^{-1}(U_x) = h^{-1}(f_2^{-1}(U_x)) ,$$

because $f_1^{-1}(U_x) = (f_2 \circ h)^{-1}(U_x) = h^{-1}(f_2^{-1}(U_x))$. So $h^{-1}(f_2^{-1}(U_x))$ is affine and equal to B_x, where B_x is a projective separable A_x-algebra. Since this holds for any $x \in X$, we have that h is finite étale.

Let now $f_1 : Y \to X$ and $f_2 : Z \to X$ be arbitrary finite étale coverings. In particular, $f_1 = f_2 \circ h$ and f_2 are affine. Then, by lemma 2.2.50, h is affine. By proposition 2.2.43, there exist two schemes W_1 and W_2 with two surjective, finite and locally free morphisms $g_1 : W_1 \to X$ and $g_2 : W_2 \to X$ such that the projections $p_{12} : Y \times_X W_1 \to W_1$ and $p_{22} : Z \times_X W_2 \to W_2$ are totally split. Let $p_{11} : Y \times_X W_1 \to Y$ and $p_{21} : Z \times_X W_2 \to Z$ be the other two projections. Then $f_1 \circ p_{11} = g_1 \circ p_{12}$ and $f_2 \circ p_{21} = g_2 \circ p_{22}$. Define $W := W_1 \times_X W_2$ and let $p_1 : W = W_1 \times_X W_2 \to W_1$ and $p_2 : W = W_1 \times_X W_2 \to W_2$ be the projections. Define also $g := g_1 \circ p_1$. Since g_1 and g_2 are surjective, finite and locally free, by lemma 2.2.32(1)-(2) we have that $g = g_1 \circ p_1 = g_2 \circ p_2$ is also surjective, finite and locally free. Consider also $(Y \times_X W_1) \times_{W_1} W$, with projections $q_1 : (Y \times_X W_1) \times_{W_1} W \to Y \times_X W_1$ and

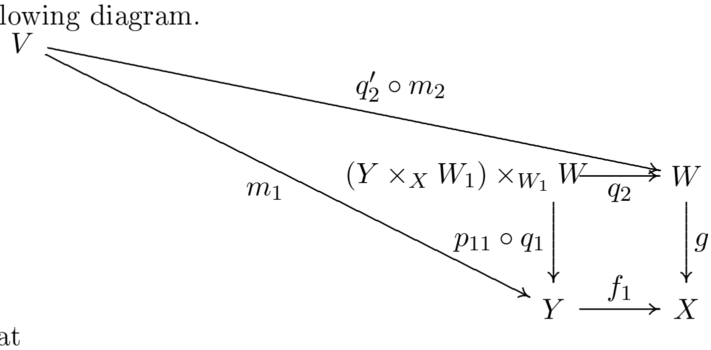
$q_2 : (Y \times_X W_1) \times_{W_1} W \to W$ (then $p_{12} \circ q_1 = p_1 \circ q_2$), and $(Z \times_X W_2) \times_{W_2} W$, with projections $q_1' : (Z \times_X W_2) \times_{W_2} W \to Z \times_X W_2$ and $q_2' : (Z \times_X W_2) \times_{W_2} W \to W$ (then $p_{22} \circ q_1' = p_2 \circ q_2'$). By lemma 2.2.41, we have that q_2 and q_2' are totally split morphisms. As in remark 2.2.44(4), one can check that $(Z \times_X W_2) \times_{W_2} W$, together with the morphisms $p_{21} \circ q_1' : (Z \times_X W_2) \times_{W_2} W \to Z$ and $q_2' : (Z \times_X W_2) \times_{W_2} W \to W$, is the fibred product of Z and W over X. Then, since g is surjective, finite and locally free, we have that $p_{21} \circ q_1' : (Z \times_X W_2) \times_{W_2} W \to Z$ is surjective, finite and locally free by lemma 2.2.28(1),(3) (applied with $g : W \to X$ instead of f and $f_2 : Z \to X$ instead of g, so that $p_{21} \circ q_1'$ plays the role of p_2). Consider moreover the following diagram.



We have that

$$f_2 \circ h \circ p_{11} \circ q_1 = f_1 \circ p_{11} \circ q_1 = g_1 \circ p_{12} \circ q_1 = g_1 \circ p_1 \circ q_2 = g \circ q_2 .$$

So the diagram is commutative. By the universal property of the fibred product, there exists a unique morphism $\eta : (Y \times_X W_1) \times_{W_1} W \to (Z \times_X W_2) \times_{W_2} W$ such that $p_{21} \circ q_1' \circ \eta = h \circ p_{11} \circ q_1$ and $q_2' \circ \eta = q_2$. Since q_2 and q_2' are totally split, the last condition implies that η is finite étale, by what we proved above. Consider now $(Y \times_X W_1) \times_{W_1} W$, together with the morphisms $p_{11} \circ q_1 : (Y \times_X W_1) \times_{W_1} W \to Y$ and $\eta : (Y \times_X W_1) \times_{W_1} W \to (Z \times_X W_2) \times_{W_2} W$. We know that $h \circ (p_{11} \circ q_1) = (p_{21} \circ q_1') \circ \eta$. Let V be a scheme with two morphisms $m_1 : V \to Y$, $m_2 : V \to (Z \times_X W_2) \times_{W_2} W$ such that $h \circ m_1 = p_{21} \circ q_1' \circ m_2$. As in remark 2.2.44(4), one can check that $(Y \times_X W_1) \times_{W_1} W$, together with the morphisms $p_{11} \circ q_1 : (Y \times_X W_1) \times_{W_1} W \to Y$ and $q_2 : (Y \times_X W_1) \times_{W_1} W \to W$, is the fibred product of Y and W over X. Consider then the following diagram.



We have that

$$g \circ q_2' \circ m_2 = g_2 \circ p_2 \circ q_2' \circ m_2 = g_2 \circ p_{22} \circ q_1' \circ m_2 = f_2 \circ p_{21} \circ q_1' \circ m_2 = f_2 \circ h \circ m_1 = f_1 \circ m_1 .$$

So the diagram is commutative. By the universal property of the fibred product, there exists a unique morphism $m : V \to (Y \times_X W_1) \times_{W_1} W$ such that $p_{11} \circ q_1 \circ m = m_1$

and $q_2 \circ m = q_2' \circ m_2$. We have that

$$p_{21} \circ q_1' \circ \eta \circ m = h \circ p_{11} \circ q_1 \circ m = h \circ m_1 = p_{21} \circ q_1' \circ m_2$$

and

$$p_{22} \circ q_1' \circ \eta \circ m = p_2 \circ q_2' \circ \eta \circ m = p_2 \circ q_2 \circ m = p_2 \circ q_2' \circ m_2 = p_{22} \circ q_1' \circ m_2 \ .$$

By uniqueness in the universal property of the fibred product, this implies that $q_1' \circ \eta \circ m = q_1' \circ m_2$. Moreover, we have that $q_2' \circ \eta \circ m = q_2 \circ m = q_2' \circ m_2$. By uniqueness in the universal property of the fibred product, it follows that $\eta \circ m = m_2$. We already know that $p_{11} \circ q_1 \circ m = m_1$. Let now $\widetilde{m} : V \to (Y \times_X W_1) \times_{W_1} W$ be another morphism of schemes such that $p_{11} \circ q_1 \circ \widetilde{m} = m_1$ and $\eta \circ \widetilde{m} = m_2$. Then

$$q_2 \circ \widetilde{m} = q_2' \circ \eta \circ \widetilde{m} = q_2' \circ m_2 \ .$$

Since we have also that $p_{11} \circ q_1 \circ \widetilde{m} = m_1$, by definition of m we get $\widetilde{m} = m$. This shows that $(Y \times_X W_1) \times_{W_1} W$, together with the morphisms $p_{11} \circ q_1 : (Y \times_X W_1) \times_{W_1} W \to Y$ and $\eta : (Y \times_X W_1) \times_{W_1} W \to (Z \times_X W_2) \times_{W_2} W$, is the fibred product of Y and $(Z \times_X W_2) \times_{W_2} W$ over Z. We know that $p_{21} \circ q_1' : (Z \times_X W_2) \times_{W_2} W \to Z$ is surjective, finite and locally free and that η is finite étale. Then, since h is affine, by proposition 2.2.43 (with Z instead of X and $(Z \times_X W_2) \times_{W_2} W$ instead of W) we have that h is finite étale. □

Remark 2.2.52. A similar result holds for finite coverings of topological spaces: if $f : Y \to X$ and $g : Z \to X$ are finite coverings of a topological space X and $h : Y \to Z$ is a morphism of coverings from f to g, then h is a finite covering of Z. Indeed, let $z \in Z$ and consider $x := g(z) \in X$. By lemma 1.5 of the appendix, there exists an open neighbourhood U of x in X such that f, g and h are trivial above U. Then there exist finite discrete topological spaces D and E, homeomorphisms $\alpha : f^{-1}(U) \to U \times D$ and $\beta : g^{-1}(U) \to U \times E$ and a map $\varphi : D \to E$ such that $p_U \circ \alpha = f$, $q_U \circ \beta = g$, $q_U \circ (\mathrm{id}_U \times \varphi) = p_U$ and $h_{|_{f^{-1}(U)}} = \beta^{-1} \circ (\mathrm{id}_U \times \varphi) \circ \alpha$, where $p_U : U \times D \to U$ and $q_U : U \times E$ are the projections on the first factor. Since $g(z) = x \in U$, we have that $z \in g^{-1}(U)$. Then we can consider $\beta(z) \in U \times E$. Let $e \in E$ be such that $\beta(z) = (q_U(\beta(z)), e) = (g(z), e) = (x, e)$ and define $V := \beta^{-1}(U \times \{e\}) \subseteq g^{-1}(U)$. Since E has the discrete topology, we have that $U \times \{e\}$ is open in $U \times E$. Then, since β is continuous, V is open in $g^{-1}(U)$. Since g is continuous and U is open in X, we have that $g^{-1}(U)$ is open in Z. So V is open in Z. Moreover, we have that $\beta(z) = (x, e) \in U \times \{e\}$, so $z \in \beta^{-1}(U \times \{e\}) = V$. Then V is an open neighbourhood of z in Z. Since h is a morphism of coverings from f to g, we have that $f = g \circ h$. Then $h^{-1}(V) \subseteq h^{-1}(g^{-1}(U)) = f^{-1}(U)$. Since $h_{|_{f^{-1}(U)}} = \beta^{-1} \circ (\mathrm{id}_U \times \varphi) \circ \alpha$, we have that

$$\begin{aligned} h^{-1}(V) = \alpha^{-1}((\mathrm{id}_U \times \varphi)^{-1}(\beta(V))) = \\ = \alpha^{-1}((\mathrm{id}_U \times \varphi)^{-1}(U \times \{e\})) = \alpha^{-1}(U \times \varphi^{-1}(\{e\})) \end{aligned}$$

(we used the fact that $V = \beta^{-1}(U \times \{e\})$ and that β is bijective). Then, restricting α to $h^{-1}(V)$, we get a homeomorphism $\alpha : h^{-1}(V) = \alpha^{-1}(U \times \varphi^{-1}(\{e\})) \to U \times$

$\varphi^{-1}(\{e\})$. Consider now $\vartheta : U \to U \times \{e\}$, $u \mapsto (u, e)$, which is a continuous bijection. We have that $\vartheta^{-1} = q_U : U \times \{e\} \to U$ is also continuous, so ϑ is a homeomorphism. Moreover, restricting β to V, we get a homeomorphism $\beta : V = \beta^{-1}(U \times \{e\}) \to U \times \{e\}$. Them $\beta^{-1} \circ \vartheta : U \to V$ is a homeomorphism. It induces a homeomorphism $(\beta^{-1} \circ \vartheta) \times \mathrm{id}_{\varphi^{-1}(\{e\})} : U \times \varphi^{-1}(\{e\}) \to V \times \varphi^{-1}(\{e\})$. So the composition $((\beta^{-1} \circ \vartheta) \times \mathrm{id}_{\varphi^{-1}(\{e\})}) \circ \alpha : h^{-1}(V) \to V \times \varphi^{-1}(\{e\})$ is also a homeomorphism. Denote by $p_V : V \times \varphi^{-1}(\{e\}) \to V$ the projection on the first factor. Then $p_V \circ ((\beta^{-1} \circ \vartheta) \times \mathrm{id}_{\varphi^{-1}(\{e\})}) = \beta^{-1} \circ \vartheta \circ p_U$. So we have that

$$\begin{aligned} p_V \circ (((\beta^{-1} \circ \vartheta) \times \mathrm{id}_{\varphi^{-1}(\{e\})}) \circ \alpha) &= \beta^{-1} \circ \vartheta \circ p_U \circ \alpha = \beta^{-1} \circ \vartheta \circ f = \\ &= \beta^{-1} \circ \vartheta \circ g \circ h = \beta^{-1} \circ \vartheta \circ q_U \circ \beta \circ h = \beta^{-1} \circ \vartheta \circ \vartheta^{-1} \circ \beta \circ h = h \end{aligned}$$

(we applied the fact that $h(h^{-1}(V)) \subseteq V \subseteq g^{-1}(V)$ and that on $g^1(V)$ we have $g = q_U \circ \beta$). This shows that $h : h^{-1}(V) \to V$ is a trivial covering. Moreover, it is finite, because $\varphi^{-1}(\{e\}) \subseteq D$ is finite. Hence h is a finite covering of Z.
Notice that the lemma 1.7(1) of the appendix is now a consequence of this remark, together with remark 2.2.27. Notice also that, with this remark, we can give an alternative proof of the existence of the fibred product in the category $\mathbf{Cov}_X$, for a given topological space X (this is the same approach that we will use in order to prove the existence of the fibred product in the category $\mathbf{FEt}_X$, for any scheme X; see lemma 2.2.54). Indeed, if $f_1 : Y_1 \to X$, $f_2 : Y_2 \to X$ and $g : Z \to X$ are finite coverings of X, with morphisms of coverings $h_1 : Y_1 \to Z$ and $h_2 : Y_2 \to Z$, then h_1 and h_2 are finite coverings of Z and so, by remark 2.2.33, $h_1 \circ p_1 = h_2 \circ p_2 : Y_1 \times_Z Y_2 \to Z$ is also a finite covering of Z, where $p_1 : Y_1 \times_Z Y_2 \to Y_1$ and $p_2 : Y_1 \times_Z Y_2 \to Y_2$ are the two projections. Then, by remark 2.2.31, the composition $g \circ h_1 \circ p_1 = f_1 \circ p_1 : Y_1 \times_Z Y_2 \to X$ is a finite covering of X. One can show that $f_1 \circ p_1$ is the fibred product of f_1 and f_2 over g in $\mathbf{Cov}_X$ in the same way as we did in the proof of (G1) in the proposition 1.8 of the appendix.

Lemma 2.2.53. *Let X, Y and Z be schemes and let $f : Y \to X$, $g : Z \to X$ be finite étale coverings of X. A morphism of coverings $h : Y \to Z$ from f to g is an epimorphism in $\mathbf{FEt}_X$ if and only if it is surjective.*

Proof. Assume that h is an epimorphism in $\mathbf{FEt}_X$. By lemma 2.2.51, h is finite étale. Then, by corollary 2.2.26, we have that $h(Y) = \{z \in \mathrm{sp}(Z) \mid [Y : Z](z) \geq 1\}$ is open and closed in Z. Define $Z' := Z \backslash h(Y)$. Then $h(Y)$ and Z' are both open subschemes of Z and $Z = h(Y) \amalg Z'$. Consider the restrictions $g'' := g_{|h(Y)} : h(Y) \to X$ and $g' := g_{|Y'} : Y' \to X$. Since g is finite étale, by lemma 2.2.18(3) we have that g' and g'' are also finite étale. Consider now $h(Y) \amalg Z' \amalg Z'$ and let $\widetilde{g} : h(Y) \amalg Z' \amalg Z' \to X$ be the morphism obtained by gluing g'' and twice g'. Applying again lemma 2.2.18(3), we get that $\widetilde{g}$ is finite étale. Then $\widetilde{g}$ is an element of $\mathbf{Cov}_X$. Let $\iota'' : h(Y) \to h(Y) \amalg Z' \amalg Z'$, $\iota'_1 : Z' \to h(Y) \amalg Z' \amalg Z'$ and $\iota'_2 : Z' \to h(Y) \amalg Z' \amalg Z'$ be the canonical inclusions. Then, by definition of $\widetilde{g}$, we have that $\widetilde{g} \circ \iota'' = g''$ and $\widetilde{g} \circ \iota'_1 = g' = \widetilde{g} \circ \iota'_2$. Gluing ι'' and ι'_1, we get a morphism of schemes $m_1 : h(Y) \amalg Z' = Z \to h(Y) \amalg Z' \amalg Z'$. We have that

$$(\widetilde{g} \circ m_1)_{|h(Y)} = \widetilde{g} \circ \iota'' = g'' = g_{|h(Y)}$$

and

$$(\widetilde{g} \circ m_1)_{|_{Y'}} = \widetilde{g} \circ \iota'_1 = g' = g_{|_{Y'}} .$$

So $\widetilde{g} \circ m_1 = g$, which means that m_1 is a morphism of coverings from g to $\widetilde{g}$. Analogously, gluing ι'' and ι'_2, we get a morphism of schemes $m_2 : h(Y) \amalg Z' = Z \to h(Y) \amalg Z' \amalg Z'$ and we have that

$$(\widetilde{g} \circ m_2)_{|_{h(Y)}} = \widetilde{g} \circ \iota'' = g'' = g_{|_{h(Y)}}$$

and

$$(\widetilde{g} \circ m_2)_{|_{Y'}} = \widetilde{g} \circ \iota'_2 = g' = g_{|_{Y'}} .$$

So $\widetilde{g} \circ m_2 = g$, which means that m_2 is a morphism of coverings from g to $\widetilde{g}$. Now we have that

$$m_1 \circ h = (m_1)_{|_{h(Y)}} \circ h = \iota'' \circ h = (m_2)_{|_{h(Y)}} \circ h = m_2 \circ h .$$

Since h is an epimorphism in $\mathbf{FEt}_X$, this implies that $m_1 = m_2$. Then $\iota'_1 = (m_1)_{|_{Z'}} = (m_2)_{|_{Z'}} = \iota'_2$, which is possible only if $Z' = \emptyset$. Then, since $Z' = Z \backslash h(Y)$, we have that $h(Y) = Z$, i.e. h is surjective.
Conversely, assume that h is surjective and let W be a scheme with a finite étale covering $l : W \to X$ and two morphism of coverings $m_1, m_2 : Z \to W$ from g to l such that $m_1 \circ h = m_2 \circ h$. Let $z \in Z$ and consider $x := g(z) \in X$. By definition of scheme, there exists an open affine subset $U = \mathrm{Spec}(A)$ of X such that $x \in U$. Since $g(z) = x \in U$, we have that $z \in g^{-1}(U)$. Moreover, $g^{-1}(U)$ is open in Z, because U is open in X and g is continuous. So $g^{-1}(U)$ is an open neighbourhood of z in Z. Since f, g and l are finite étale, they are in particular affine. Then, by lemma 2.2.10(1) we have that $f^{-1}(U)$, $g^{-1}(U)$ and $l^{-1}(U)$ are all affine. Let B, C and D be rings such that $f^{-1}(U) = \mathrm{Spec}(B)$, $g^{-1}(U) = \mathrm{Spec}(C)$ and $l^{-1}(U) = \mathrm{Spec}(D)$. Since m_1 and m_2 are morphisms of coverings from g to l, we have that $l \circ m_1 = g = l \circ m_2$. Then $g^{-1}(U) = (l \circ m_1)^{-1}(U) = m_1^{-1}(l^{-1}(U))$, which implies that $m_1(g^{-1}(U)) \subseteq l^{-1}(U)$, and $g^{-1}(U) = (l \circ m_2)^{-1}(U) = m_2^{-1}(l^{-1}(U))$, which implies that $m_2(g^{-1}(U)) \subseteq l^{-1}(U)$. So, restricting m_1 and m_2 to $g^{-1}(U)$, we get two morphisms of schemes from $g^{-1}(U) = \mathrm{Spec}(C)$ to $l^{-1}(U) = \mathrm{Spec}(D)$. Let $m_1^{\#}, m_2^{\#} : D \to C$ be the corresponding ring homomorphisms. Analogously, since h is a morphism of coverings from f to g, we have that $f = g \circ h$ and so $f^{-1}(U) = (g \circ h)^{-1}(U) = h^{-1}(g^{-1}(U))$, which implies that $h(f^{-1}(U)) \subseteq g^{-1}(U)$. So, restricting h to $f^{-1}(U)$, we get a morphism of schemes from $f^{-1}(U) = \mathrm{Spec}(B)$ to $g^{-1}(U) = \mathrm{Spec}(C)$. Consider the corresponding ring homomorphism $h^{\#} : C \to D$. Since $m_1 \circ h = m_2 \circ h$, we have that $h^{\#} \circ m_1^{\#} = h^{\#} \circ m_2^{\#}$. By lemma 2.2.51, we have that h is finite étale. Then, since $\mathrm{Spec}(B) = f^{-1}(U) = h^{-1}(g^{-1}(U)) = h^{-1}(\mathrm{Spec}(C))$, we have that B is a projective separable C-algebra (with the C-algebra structure induced by $h^{\#}$). In particular, B is a finite projective C-algebra. By assumption h is surjective, so $[Y : Z] \geq 1$ by lemma 2.2.15(3). By definition of degree, we have that $[Y : Z]_{|_{g^{-1}(U)}} = d_{g^{-1}(U)} = [B : C]$ (see lemma 2.2.12). So $[B : C] \geq 1$, which by lemma 2.1.58(1) implies that $h^{\#}$ is injective. Then $h^{\#}$ is a monomorphism of sets (example 1.1.3(6); notice that in that proof we did not use the finiteness of the

involved sets). Now from $h^{\#} \circ m_1^{\#} = h^{\#} \circ m_2^{\#}$ it follows that $m_1^{\#} = m_2^{\#}$ and so also the corresponding morphisms of schemes coincide, i.e. $(m_1)_{|_{g^{-1}(U)}} = (m_2)_{|_{g^{-1}(U)}}$. So we have proved that, for any $z \in Z$, there exists an open neighbourhood V of z in Z such that $(m_1)_{|_V} = (m_2)_{|_V}$. This implies that $m_1 = m_2$. Hence h is an epimorphism. □

Lemma 2.2.54. *Let X, Y_1, Y_2 and Z be schemes, $f_1 : Y_1 \to X$, $f_2 : Y_2 \to X$ and $g : Z \to X$ finite étale coverings of X and $h_1 : Y_1 \to Z$, $h_2 : Y_2 \to Z$ two morphisms of coverings. Consider the fibred product $Y_1 \times_Z Y_2$, with projections $p_1 : Y_1 \times_Z Y_2 \to Y_1$ and $p_2 : Y_1 \times_Z Y_2 \to Y_2$. Define $f := f_1 \circ p_1 : Y_1 \times_Z Y_2 \to X$. Then f is a finite étale covering of X and it is the fibred product of f_1 and f_2 over g in $\mathbf{FEt}_X$.*

Proof. By lemma 2.2.51, we have that h_1 and h_2 are finite étale. Then, by lemma 2.2.32(3), we have that $h_1 \circ p_1 = h_2 \circ p_2 : Y_1 \times_Z Y_2 \to Z$ is finite étale. Since h_1 is a morphism of coverings from f_1 to g, we have that $f_1 = g \circ h_1$. Then $f = f_1 \circ p_1 = g \circ h_1 \circ p_1$. By lemma 2.2.30, it follows that f is finite étale, because g and $h_1 \circ p_1$ are finite étale. So $f : Y_1 \times_Z Y_2 \to X$ is an object of $\mathbf{FEt}_X$. Since $f = f_1 \circ p_1$, we have that p_1 is a morphism of coverings from f to f_1. Moreover, since h_2 is a morphism of coverings from f_2 to g, we have that $f_2 = g \circ h_2$ and so $f = g \circ h_1 \circ p_1 = g \circ h_2 \circ p_2 = f_2 \circ p_2$. This shows that p_2 is a morphism of coverings from f to f_2. We already know that $h_1 \circ p_1 = h_2 \circ p_2$ (by definition of fibred product). Let now W be a scheme and $l : W \to X$ a finite étale covering of X, with two morphisms of coverings $m_1 : W \to Y_1$, $m_2 : W \to Y_2$ such that $h_1 \circ m_1 = h_2 \circ m_2$. By the universal property of the fibred product in the category of schemes, there exist a unique morphism of schemes $m : W \to Y_1 \times_Z Y_2$ such that $m_1 = p_1 \circ m$ and $m_2 = p_2 \circ m$. Since m_1 is a morphism of coverings from l to f_1, we have that $l = f_1 \circ m_1$ and then $f \circ m = f_1 \circ p_1 \circ m = f_1 \circ m_1 = l$. So m is a morphism of coverings from l to f. This ends the proof. □

Lemma 2.2.55. *Let X and Y be schemes, $f : X \to Y$ a morphism of schemes. If $f(X)$ is open in Y and $f : X \to f(X)$ is an isomorphism of schemes, then f is a monomorphism in the category* **Sch** *of all schemes.*

Proof. Notice that, since $f(X)$ is open, it has a natural subscheme structure and we can see f as a morphism of schemes from X to $f(X)$. Since $f : X \to f(X)$ is an isomorphism, we can consider the inverse morphism $f^{-1} : f(X) \to X$. Let now Z be a scheme with two morphisms $g, h : Z \to X$ such that $f \circ g = f \circ h$. Since $(f \circ g)(Z) = (f \circ h)(Z) \subseteq f(X)$, we can see $f \circ g = f \circ h$ as a morphism from Z to $f(X)$. Then we can compose it with f^{-1} and get

$$g = f^{-1} \circ f \circ g = f^{-1} \circ f \circ h = h \, .$$

This proves that h is a monomorphism in **Sch**. □

Lemma 2.2.56. *Let X, Y and Z be schemes and let $f : Y \to X$, $g : Z \to X$ be finite étale coverings of X. A morphism of coverings $h : Y \to Z$ from f to g is an monomorphism in $\mathbf{FEt}_X$ if and only if $h : Y \to h(Y)$ is an isomorphism of schemes.*

Proof. First of all, notice that, by lemma 2.2.51, h is finite étale. Then, by corollary 2.2.26, we have that $h(Y) = \{z \in \mathrm{sp}(Z) \mid [Y : Z](z) \geq 1\}$ is open and closed in Z. In particular, since $h(Y)$ is open in Z, it has a natural subscheme structure and $h : Y \to h(Y)$ is a morphism of scheme.
Assume now that $h : Y \to h(Y)$ is an isomorphism of schemes. Then, by lemma 2.2.55, we have that h is a monomorphism in **Sch**. Let W be a scheme with a finite étale covering $l : W \to X$ and two morphism of coverings $m_1, m_2 : W \to Y$ from l to f such that $h \circ m_1 = h \circ m_2$. In particular, m_1 and m_2 are morphisms of schemes. Then, since h is a monomorphism of schemes, we must have $m_1 = m_2$. This proves that h is a monomorphism in $\mathbf{FEt}_X$
Conversely, assume that h is a monomorphism in $\mathbf{FEt}_X$. Consider the fibred product $Y \times_Z Y$, with projections $p_1 : Y \times_Z Y \to Y$ and $p_2 : Y \times_Z Y \to Y$. By lemma 2.2.54, we have that $f \circ p_1 : Y \times_Z Y \to X$, together with the projections p_1 and p_2, is the fibred product of f with itself over g in $\mathbf{FEt}_X$. Then, since h is a monomorphism in $\mathbf{FEt}_X$, by lemma 1.2.9 we have that $p_1 : Y \times_Z Y \to Y$ is an isomorphism in $\mathbf{FEt}_X$ (notice that the only axiom that we used to prove that lemma was the existence of fibred products). In particular, p_1 is an isomorphism of schemes. Let $z \in Z$ and consider $x := g(z) \in X$. By definition of scheme, there exists an open affine subset $U = \mathrm{Spec}(A)$ of X such that $x \in U$. Then $z \in g^{-1}(U)$. Since f and g are finite étale, they are in particular affine. Then, by lemma 2.2.10(1), we have that $f^{-1}(U)$ and $g^{-1}(U)$ are both affine. Let B and C be rings such that $f^{-1}(U) = \mathrm{Spec}(B)$ and $g^{-1}(U) = \mathrm{Spec}(C)$. Since h is a morphism of coverings, we have that $f = g \circ h$ and so $\mathrm{Spec}(B) = f^{-1}(U) = (g \circ h)^{-1}(U) = h^{-1}(g^{-1}(U)) = h^{-1}(\mathrm{Spec}(C))$. Since h is finite étale, this implies that B is a projective separable C-algebra. In particular, it is a finite projective C-algebra. Consider now $p_1^{-1}(f^{-1}(U)) \subseteq Y \times_Z Y$. As in the proof of lemma 2.2.34, we have that

$$\begin{aligned} p_1^{-1}(f^{-1}(U)) &= p_1^{-1}(h^{-1}(g^{-1}(U))) = h^{-1}(g^{-1}(U)) \times_{g^{-1}(U)} h^{-1}(g^{-1}(U)) = \\ &= f^{-1}(U) \times_{g^{-1}(U)} f^{-1}(U) = \mathrm{Spec}(B) \times_{\mathrm{Spec}(C)} \mathrm{Spec}(B) = \mathrm{Spec}(B \otimes_C B) \; . \end{aligned}$$

Since p_1 is an isomorphism, its restriction $p_1 : p_1^{-1}(f^{-1}(U)) = \mathrm{Spec}(B \otimes_C B) \to f^{-1}(U) = \mathrm{Spec}(B)$ is also an isomorphism. Then the corresponding ring homomorphism $p_1^{\#} : B \to B \otimes_C B$ is also an isomorphism. But $p_1^{\#}$ is defined by $p_1^{\#}(x) = x \otimes 1$ for any $x \in B$. Let $m : B \otimes_C B \to B$, $x \otimes y \mapsto xy$, extended by linearity, as in lemma 2.1.58(2). We have that $(m \circ p_1^{\#})(x) = m(x \otimes 1) = x \cdot 1 = x = \mathrm{id}_B(x)$ for any $x \in B$. So $m \circ p_1^{\#} = \mathrm{id}_B$. Since $p_1^{\#}$ is invertible, this implies that $m = (p_1^{\#})^{-1}$. In particular, m is invertible and so it is an isomorphism of C-algebras. By lemma 2.1.58(2), it follows that $[B : C] \leq 1$. Then, by definition of degree (see lemma 2.2.12), we have that

$$[Y : Z](z) = d_{g^{-1}(U)}(z) = [B : C](z) \leq 1 \; ,$$

because $z \in g^{-1}(U) = \mathrm{Spec}(C)$. This shows that $[Y : Z] \leq 1$. We have that $Y = h^{-1}(h(Y))$ and then, by lemma 2.2.22, $h : Y = h^{-1}(h(Y)) \to h(Y)$ is finite étale, with degree $[Y : h(Y)] = [Y : Z]_{|_{h(Y)}}$. Since $h(Y) = \{z \in \mathrm{sp}(Z) \mid [Y : Z](z) \geq 1\}$, we have that $[Y : Z]_{|_{h(Y)}} \geq 1$. But we have proved that $[Y : Z] \leq 1$, so $[Y : Z]_{|_{h(Y)}} \leq 1$. Then $[Y : h(Y)] = [Y : Z]_{|_{h(Y)}} = 1$. By lemma 2.2.15(2), $h : Y \to h(Y)$ is an isomorphism. $\square$

We omit the proof of the following two results, which can be found in [1],5.18-21. We just mention that the main idea is to show that, for any scheme X, quotients by finite groups of automorphisms exist in the category $\mathbf{Aff}_X$ whose objects are affine morphisms $Y \to X$ and whose morphisms are defined in an analogous way to morphisms of finite étale coverings (i.e., if $f : Y \to X$ and $g : Z \to X$ are affine morphisms, a morphism between them is a morphism of schemes $h : Y \to Z$ such that $f = g \circ h$) and then to prove that the full subcategory $\mathbf{FEt}_X$ is closed with respect to quotients.

Proposition 2.2.57. *For any scheme X, quotients by finite groups of automorphisms exist in $\mathbf{FEt}_X$.*

Lemma 2.2.58. *Let X, Y and Z be schemes, $f : Y \to X$ a finite étale morphism, G a finite group of automorphisms of f in $\mathbf{FEt}_X$ and $g : Z \to X$ any morphism of schemes. Then $(Y \times_X Z)/G \cong (Y/G) \times_X Z$ in $\mathbf{FEt}_Z$.*

2.3 The main theorem of Galois theory for schemes

We want now to define a functor $\mathbf{FEt}_X \to \mathbf{sets}$, which will be the fundamental functor of our Galois category. We will actually have many fundamental functors, one for each geometric point of X. Recall the following definition.

Definition 2.3.1. Let X be a scheme. A *geometric point* of X is a morphism of schemes $x : \mathrm{Spec}(\Omega) \to X$, where Ω is an algebraically closed field.

Remark 2.3.2. If X is a scheme and $a \in \mathrm{sp}(X)$, then we can define a geometric point of X as follows. Let $\kappa(a) = \mathcal{O}_{X,a}/\mathfrak{m}_{X,a}$ be the residue field at a and let Ω be an algebraic closure of $\kappa(a)$. So Ω is algebraically closed and $\kappa(a) \subseteq \Omega$. Consider the map $x : \mathrm{Spec}(\Omega) \to \mathrm{sp}(X)$, $0 \mapsto a$, which is continuous because it is constant. Let U be an open subset of X. If $a \notin U$, then $x_*\mathcal{O}_{\mathrm{Spec}(\Omega)}(U) = \mathcal{O}_{\mathrm{Spec}(\Omega)}(x^{-1}(U)) = \mathcal{O}_{\mathrm{Spec}(\Omega)}(\emptyset) = 0$. Then we define $x^\# : \mathcal{O}_X(U) \to x_*\mathcal{O}_{\mathrm{Spec}(\Omega)}(U) = 0$ to be the zero map. If instead $a \in U$, then $x_*\mathcal{O}_{\mathrm{Spec}(\Omega)}(U) = \mathcal{O}_{\mathrm{Spec}(\Omega)}(x^{-1}(U)) = \mathcal{O}_{\mathrm{Spec}(\Omega)}(\mathrm{Spec}(\Omega)) = \Omega$. We have a natural ring homomorphism $\mathcal{O}_X(U) \to \mathcal{O}_{X,a}$, which composed with the canonical projection $\mathcal{O}_{X,a} \to \kappa(a) = \mathcal{O}_{X,a}/\mathfrak{m}_{X,a}$ gives a ring homomorphism $\mathcal{O}_X(U) \to \kappa(a)$. Since $\kappa(a) \subseteq \Omega$, we can define $x^\# : \mathcal{O}_X(U) \to x_*\mathcal{O}_{\mathrm{Spec}(\Omega)}(U) = \Omega$. It is immediate to check that these definitions give a morphism of schemes $x : \mathrm{Spec}(\Omega) \to X$.
So any non-empty scheme has at least one geometric point. In particular this is true for any connected scheme (recall that we do not consider the empy scheme as a connected scheme).

Given a geometric point $x : \mathrm{Spec}(\Omega) \to X$, we associate to any finite étale covering of X the set of morphisms from x to f in $\mathbf{Sch}_X$, i.e. $\mathrm{Hom}_{\mathbf{Sch}_X}(x, f) = \{y : \mathrm{Spec}(\Omega) \to Y \mid f \circ y = x\}$. It is however not clear that this is a finite set. In order to prove this, we start with the case when $X = \mathrm{Spec}(\Omega)$ and $x = \mathrm{id}_{\mathrm{Spec}(\Omega)}$. We need an algebraic preparation.

Lemma 2.3.3. *Let K be a field and A a finite-dimensional K-algebra. Then there exist $n \in \mathbb{Z}_{\geq 0}$ and some local K-algebras $A_1, \dots, A_n$ with nilpotent maximal ideals such that $A \cong \prod_{i=1}^n A_i$.*

Proof. Let $\mathfrak{p}$ be a prime ideal of A. We have that $A/\mathfrak{p}$ has an induced K-algebra structure and, since A is finite-dimensional, $A/\mathfrak{p}$ is also finite dimensional (it is generated by $(a_1+\mathfrak{p},\dots,a_n+\mathfrak{p})$, if $(a_1,\dots,a_n)$ generates A over K). Let $x\in(A/\mathfrak{p})\setminus\{0\}$ and consider the map $m_x: A_\mathfrak{p}\to A_\mathfrak{p},\ y\mapsto xy$, which is K-linear. Let $y\in\mathrm{Ker}(m_x)$, i.e. $xy=m_x(y)=0$. Since $\mathfrak{p}$ is prime, $A/\mathfrak{p}$ is an integral domain. Then we must have $y=0$. So $\mathrm{Ker}(m_x)=0$, i.e. m_x is injective. Since $A/\mathfrak{p}$ is finite dimensional, m_x is also surjective. Then there exists $y\in A/\mathfrak{p}$ such that $xy=1$. So x is a unit of $A/\mathfrak{p}$ and, since this holds for any $x\in A/\mathfrak{p}\setminus\{0\}$, we have that $A/\mathfrak{p}$ is a field. Then $\mathfrak{p}$ is a maximal ideal. This shows that any prime ideal of A is maximal. Let now $\mathfrak{m}_1,\dots,\mathfrak{m}_n$ be pairwise distinct maximal ideals of A. Then $\mathfrak{m}_1,\dots,\mathfrak{m}_n$ are coprime with each other. By the Chinese remainder theorem, the ring homomorphism $A\to\prod_{i=1}^n A/\mathfrak{m}_i,\ a\mapsto(a+\mathfrak{m}_1,\dots,a+\mathfrak{m}_n)$ is surjective. This ring homomorphism is also K-linear, if we consider the induced K-algebra structure on $A/\mathfrak{m}_i$ for any $i=1,\dots,n$. Then we have that

$$\dim_K(A)\geq\dim_K\left(\prod_{i=1}^n A/\mathfrak{m}_i\right)=\sum_{i=1}^n\dim_K(A/\mathfrak{m}_i)\geq\sum_{i=1}^n 1=n\ .$$

(we used the fact that, for any $i=1,\dots,n$, $A/\mathfrak{m}_i\neq 0$, because any maximal ideal is proper, and so $\dim_K(A/\mathfrak{m}_i)\geq 1$). So the number of distinct maximal ideals is bounded by $\dim_K(A)$. In particular, A has finitely many maximal ideals. Let $\mathfrak{m}_1,\dots,\mathfrak{m}_n$ be all the distinct maximal ideals of A and consider their intersection $\bigcap_{i=1}^n\mathfrak{m}_i$. Since any prime ideal is maximal, we have that $\bigcap_{i=1}^n\mathfrak{m}_i=\bigcap_{\mathfrak{p}\text{ prime}}\mathfrak{p}=\sqrt{0}$. Since A is finite-dimensional, it is also finitely generated as a K-algebra. Then $A\cong K[x_1,\dots,x_t]/I$ as K-algebras, for a $t\in\mathbb{Z}_{\geq 0}$ and an ideal I of $K[x_1,\dots,x_t]$. Since K is a field, it is noetherian. Then, by Hilbert's basis theorem, $K[x_1,\dots,x_n]$ is noetherian and so the quotient $A\cong K[x_1,\dots,x_t]/I$ is noetherian. It follows that $\sqrt{0}$ is finitely generated as an A-module. Let $(b_1,\dots,b_k)$ be generators of $\sqrt{0}$ over A. For any $i=1,\dots,k$, by definition of nilradical, there exists $m_i\geq 1$ such that $b_i^{m_i}=0$. Let $m:=\sum_{i=1}^k m_i$. For any $x\in\sqrt{0}$, there exist $a_1,\dots,a_k\in A$ such that $x=\sum_{i=1}^k a_ib_i$. Then $x^m=\left(\sum_{i=1}^k a_ib_i\right)^m=\sum_{\substack{\alpha_1+\dots+\alpha_k=m\\ \alpha_1,\dots,\alpha_k\geq 0}}\binom{m}{\alpha_1,\dots,\alpha_k}\prod_{i=1}^k(a_ib_i)^{\alpha_i}$. For any $\alpha_1,\dots,\alpha_k\geq 0$ such that $\alpha_1+\dots+\alpha_k=m$, there exists $i_0\in\{1,\dots,k\}$ such that $\alpha_{i_0}\geq m_{i_0}$ and so $b_{i_0}^{\alpha_{i_0}}=0$. Then $\prod_{i=1}^k(a_ib_i)^{\alpha_i}=0$, for any $\alpha_1,\dots,\alpha_k\geq 0$ such that $\alpha_1+\dots+\alpha_k=m$. This implies that $x^m=0$. So $\sqrt{0}^m=0$. Then we have that

$$0=\sqrt{0}^m=\left(\bigcap_{i=1}^n\mathfrak{m}_i\right)^m\supseteq\bigcap_{i=1}^n\mathfrak{m}_i^m\supseteq\prod_{i=1}^n\mathfrak{m}_i^m\ ,$$

which implies that $\prod_{i=1}^n\mathfrak{m}_i^m=0$. We claim that $\mathfrak{m}_1^m,\dots,\mathfrak{m}_n^m$ are pairwise coprime. If $\mathfrak{m}_i^m+\mathfrak{m}_j^m$ is a proper ideal of A, for some $i,j\in\{1,\dots,n\}$, there would exist a maximal ideal $\mathfrak{m}$ of A such that $\mathfrak{m}_i^m+\mathfrak{m}_j^m\subseteq\mathfrak{m}$. Then $\mathfrak{m}_i^m\subseteq\mathfrak{m}$ and $\mathfrak{m}_j^m\subseteq\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, it is in particular prime. Then we must have $\mathfrak{m}_i\subseteq\mathfrak{m}$ and $\mathfrak{m}_j\subseteq\mathfrak{m}$. Since $\mathfrak{m}_i$ and $\mathfrak{m}_j$ are maximal, this implies that $\mathfrak{m}_i=\mathfrak{m}=\mathfrak{m}_j$ and so $i=j$. So $\mathfrak{m}_1^m,\dots,\mathfrak{m}_n^m$ are pairwise coprime. Then, by the Chinese remainder theorem, the ring homomorphism $A\to\prod_{i=1}^n A/\mathfrak{m}_i^m,\ a\mapsto(a+\mathfrak{m}_1^m,\dots,a+\mathfrak{m}_n^m)$ is an isomorphism. This ring isomorphism is also K-linear, if we consider the induced K-algebra structure on $A/\mathfrak{m}_i^m$ for any $i = 1, \dots, n$. Then, if we define $A_i := A/\mathfrak{m}_i^m$ for any $i = 1, \dots, n$, we have that $A \cong \prod_{i=1}^n A_i$ as K-algebras. Moreover, for any $i = 1, \dots, n$, we have that $\mathfrak{m}_i$ is the unique maximal ideal of A that contains $\mathfrak{m}_i^m$ (because any maximal ideal is prime and so if $\mathfrak{m}_i^m \subseteq \mathfrak{m}_j$ we must have $\mathfrak{m}_i \subseteq \mathfrak{m}_j$, which implies that $\mathfrak{m}_i = \mathfrak{m}_j$ by maximality) and so, by the correspondence theorem for ideals, $\mathfrak{m}_i/\mathfrak{m}_i^m$ is the unique maximal ideal of $A/\mathfrak{m}_i^m = A_i$. Moreover, it is a nilpotent ideal, because $(\mathfrak{m}_i/\mathfrak{m}_i^m)^m = \mathfrak{m}_i^m/\mathfrak{m}_i^m = 0$. □

Lemma 2.3.4. *Let Ω be an algebraically closed field and A a projective separable Ω-algebra (A is actually free, because all vector spaces are free). Then $A \cong \Omega^n$ as Ω-algebras, for some $n \in \mathbb{Z}_{\geq 0}$.*

Proof. Since A is projective separable, it is in particular finitely generated as an Ω-vector space. Then, by lemma 2.3.3, we have that $A \cong \prod_{i=1}^n A_i$ as A-algebras, for some local K-algebras $A_1, \dots, A_n$ with nilpotent maximal ideals (and $n \in \mathbb{Z}_{\geq 0}$). Then it is enough to show that $A_i = \Omega$, for any $i = 1, \dots, n$. Since A is projective separable, by lemma 2.1.64 we have that A_i is projective separable for every $i = 1, \dots, n$. Fix $i \in \{1, \dots, n\}$ and let $\varphi_i : A_i \to \mathrm{Hom}_\Omega(A_i, \Omega)$ be defined as in lemma 2.1.59, with Ω instead of A and A_i instead of B. Let now $f \in \mathrm{Hom}_\Omega(A_i, \Omega)$. Since A_i is projective separable, we have that φ_i is an isomorphism, so there exist a (unique) $a \in A_i$ such that $f = \varphi_i(a)$. Let $x \in \mathfrak{m}_i$. Then $f(x) = \varphi_i(a)(x) = \mathrm{Tr}(ax)$. We know that $\mathfrak{m}_i$ is nilpotent, so there exists $m \geq 1$ such that $\mathfrak{m}_i^m = 0$. In particular, $x^m = 0$. Then $m_{ax}^m = m_{(ax)^m} = m_{a^m x^m} = m_0 = 0$. Then m_{ax} is nilpotent. By remark 2.1.50(3), in the case of vector spaces the trace defined in 2.1.47 is the ususal one. It is well known that the trace of a nilpotent endomorphism of a vector space is 0. Then $f(x) = \mathrm{Tr}(ax) = \mathrm{Tr}(m_{ax}) = 0$, i.e. $x \in \mathrm{Ker}(f)$. This holds for any $f \in \mathrm{Hom}_\Omega(A_i, \Omega)$. If $(a_1, \dots, a_k)$ is an Ω-basis of A_i (which is finite dimensional because A is finite dimensional), there exist $\lambda_1, \dots, \lambda_k \in \Omega$ such that $x = \lambda_1 a_1 + \dots + \lambda_k a_k$. Let $(a_1^*, \dots, a_k^*)$ be the dual basis of $(a_1, \dots, a_k)$. Then, for any $i = 1, \dots, k$, we have that $a_i^* \in \mathrm{Hom}_\Omega(A_i, \Omega)$ and, by what we proved above,

$$0 = a_i^*(x) = a_i^*\left(\sum_{j=1}^k \lambda_j a_j\right) = \sum_{j=1}^k \lambda_j a_i^*(a_j) = \sum_{j=1}^n \lambda_j \delta_{ij} = \lambda_i \, .$$

So $x = 0$. This proves that $\mathfrak{m}_i = 0$. Then A_i is a field. Since A_i is an Ω-algebra, it is a field extension of Ω. Moreover, since A_i is finite dimensional, it is an algebrical field extension. But Ω is algebraically closed. Hence $A_i = \Omega$. □

Remark 2.3.5. In [1], 2.7, a more general result is proved, classifying free separable K-algebras for any field K as finite products of finite separable field extensions of K.

Lemma 2.3.6. *Let Ω be an algebraically closed field and let $f : Y \to \mathrm{Spec}(\Omega)$ be a finite étale covering. Consider*

$$\mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, f) = \{y : \mathrm{Spec}(\Omega) \to Y \mid f \circ y = \mathrm{id}_{\mathrm{Spec}(\Omega)}\} \, .$$

We have that $|\mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, f)| = [Y : \mathrm{Spec}(\Omega)]$ *(since* $\mathrm{Spec}(\Omega)$ *is connected, the degree is constant). In particular,* $\mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, f)$ *is a finite set.*

Proof. Since f is finite étale and $\mathrm{Spec}(\Omega)$ is affine, by lemma 2.2.10(4) we have that $Y = f^{-1}(\mathrm{Spec}(\Omega))$ is affine and equal to $\mathrm{Spec}(A)$, where A is a projective separable Ω-algebra. There is a bijective correspondence between morphisms of schemes $y : \mathrm{Spec}(\Omega) \to Y = \mathrm{Spec}(A)$ such that $f \circ y = \mathrm{id}_{\mathrm{Spec}(\Omega)}$ and Ω-algebra homomorphisms $A \to \Omega$. By lemma 2.3.6, there exists $n \in \mathbb{Z}_{\geq 0}$ such that $A \cong \Omega^n$ as A-algebras. Notice that this implies that

$$n = \dim_{\Omega}(\Omega^n) = \dim_{\Omega}(A) = [A : \Omega] = [Y : \mathrm{Spec}(\Omega)] ,$$

by definition of the degree (see 2.2.12). Then we have to prove that there are exactly n homomorphisms of Ω-algebras from A (or, equivalently, from Ω^n, since $A \cong \Omega^n$) to Ω. For any $i = 1, \ldots, n$, let $p_i : \Omega^n \to \Omega$ be the i-th projection, which is an Ω-algebra homomorphism. Since $p_1, \ldots, p_n : \Omega^n \to \Omega$ are n distinct Ω-algebra homomorphisms, we have to prove that any Ω-algebra homomorphism from Ω^n to Ω is of this form. Let $f : \Omega^n \to \Omega$ be a Ω-algebra homomorphism. If $E = \{1, \ldots, n\}$ and $D = \{1\}$, we have that $\Omega^n = \Omega^E$ and $\Omega = \Omega^D$. Since Ω is a field, it has no non-trivial idempotents. Then we can apply lemma 2.2.46 and get that $f : \Omega^E \to \Omega^D$ is induced by a map $\varphi : D = \{1\} \to E = \{1, \ldots, n\}$. If $i = \varphi(1)$, we have that $f((x_1, \ldots, x_n)) = x_{\varphi(1)} = x_i = p_i((x_1, \ldots, x_n))$, for any $(x_1, \ldots, x_n) \in \Omega^n$. So $f = p_i$. □

Lemma 2.3.7. *Let X be a scheme and let $x : \mathrm{Spec}(\Omega) \to X$ be a geometric point of X. If $f : Y \to X$ is a finite étale covering of X, consider*

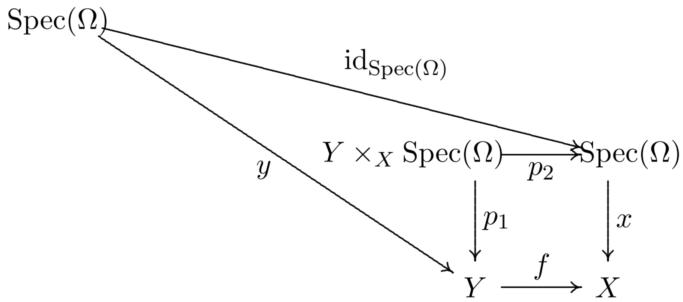
$$\mathrm{Hom}_{\mathbf{Sch}_X}(x, f) = \{y : \mathrm{Spec}(\Omega) \to Y \mid f \circ y = x\} .$$

We have that $\mathrm{Hom}_{\mathbf{Sch}_X}(x, f)$ *is a finite set. Moreover, if f has constant degree, then* $|\mathrm{Hom}_{\mathbf{Sch}_X}(x, f)| = [Y : X]$.

Proof. Consider the fibred product $Y \times_X \mathrm{Spec}(\Omega)$, with projections $p_1 : Y \times_X \mathrm{Spec}(\Omega) \to Y$ and $p_2 : Y \times_X \mathrm{Spec}(\Omega) \to \mathrm{Spec}(\Omega)$. Since f is finite étale, by lemma 2.2.28(4) we have that p_2 is a finite étale covering of $\mathrm{Spec}(\Omega)$. By lemma 2.3.6, we have that $|\mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, p_2)| = [Y \times_X \mathrm{Spec}(\Omega) : \mathrm{Spec}(\Omega)]$. We claim that $|\mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, p_2)| = |\mathrm{Hom}_{\mathbf{Sch}_X}(x, f)|$. Define

$$\varphi : \mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, p_2) \to \mathrm{Hom}_{\mathbf{Sch}_X}(x, f),\ z \mapsto p_1 \circ z$$

Let us check that φ is well defined. If $z \in \mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, p_2)$, we have that $p_2 \circ z = \mathrm{id}_{\mathrm{Spec}(\Omega)}$. By definition of fibred product, we have that $f \circ p_1 = x \circ p_2$. Then $f \circ \varphi(z) = f \circ p_1 \circ z = x \circ p_2 \circ z = x \circ \mathrm{id}_{\mathrm{Spec}(\Omega)} = x$. This proves that $\varphi(z) \in \mathrm{Hom}_{\mathbf{Sch}_X}(x, f)$. Then φ is well defined. Let now $y \in \mathrm{Hom}_{\mathbf{Sch}_X}(x, f)$. Then $f \circ y = x$. Consider the following diagram.



We have that $f \circ y = x = x \circ \mathrm{id}_{\mathrm{Spec}(\Omega)}$. So the diagram is commutative and, by the universal property of the fibred product, there exists a unique morphism $z : \mathrm{Spec}(\Omega) \to Y \times_X \mathrm{Spec}(\Omega)$ such that $p_1 \circ z = y$ and $p_2 \circ z = \mathrm{id}_{\mathrm{Spec}(\Omega)}$, i.e. a unique $z \in \mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, p_2)$ such that $\varphi(z) = p_1 \circ z = y$. This shows that φ is bijective. Then $\mathrm{Hom}_{\mathbf{Sch}_X}(x, f)$ is finite, because $\mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, p_2)$ is finite. Moreover,

$$|\mathrm{Hom}_{\mathbf{Sch}_X}(x, f)| = |\mathrm{Hom}_{\mathbf{Sch}_{\mathrm{Spec}(\Omega)}}(\mathrm{id}_{\mathrm{Spec}(\Omega)}, p_2)| = [Y \times_X \mathrm{Spec}(\Omega) : \mathrm{Spec}(\Omega)] = \\ = [Y \times_X \mathrm{Spec}(\Omega) : \mathrm{Spec}(\Omega)](0) = [Y : X](x(0))$$

(the last equality follows from lemma 2.2.28(2)). If f has constant rank, it follows that $\mathrm{Hom}_{\mathbf{Sch}_X}(x, f) = [Y : X]$. □

Lemma 2.3.8. *Let X be a scheme and $x : \mathrm{Spec}(\Omega) \to X$ a geometric point of X. For any finite étale covering $f : Y \to X$, define $F_x(f) := \mathrm{Hom}_{\mathbf{Sch}_X}(x, f)$, which is a finite set by lemma 2.3.6. Moreover, if $f : Y \to X$ and $g : Z \to X$ are finite étale coverings of X and $h : Y \to Z$ is a morphism of coverings, define $F_x(h) : F_x(f) \to F_x(g)$, $y \mapsto h \circ y$. Then $F_x : \mathbf{FEt}_X \to \mathbf{sets}$ is a functor.*

Proof. If $f : Y \to X$ and $g : Z \to X$ are finite étale coverings of X and $h : Y \to Z$ is a morphism of coverings, we have that h is in particular a morphism from f to g in $\mathbf{Sch}_X$. Then, for any $y \in F_x(f) = \mathrm{Hom}_{\mathbf{Sch}_X}(x, f)$, we have that $h \circ y \in \mathrm{Hom}_{\mathbf{Sch}_X}(x, g) = F_x(g)$. This shows that $F_x(h) : F_x(f) \to F_x(g)$ is well defined.
Moreover, if $f : Y \to X$ is a finite étale covering, we have that $F_x(\mathrm{id}_Y)(y) = \mathrm{id}_Y \circ y = y = \mathrm{id}_{F_x(f)}(y)$ for any $y \in F_x(f)$ and so $F_x(\mathrm{id}_Y) = \mathrm{id}_{F_x(f)}$. Finally, if $f_1 : Y_1 \to X$, $f_2 : Y_2 \to X$ and $f_3 : Y_3 \to X$ and finite étale coverings of X and $h_1 : Y_1 \to Y_2$, $h_2 : Y_2 \to Y_3$ are morphisms of coverings, we have that

$$F_x(h_2 \circ h_1)(y) = (h_2 \circ h_1) \circ y = h_2 \circ (h_1 \circ y) = F_x(h_2)(h_1 \circ y) = F_x(h_2)(F_x(h_1)(y))$$

for any $y \in F_x(f_1)$ and so $F_x(h_2 \circ h_1) = F_x(h_2) \circ F_x(h_1)$. Hence F_x is a functor. □

Remark 2.3.9. (1) We gave a slightly different definition of F_x in comparison with that of [1] (which relies on the result proved in 2.9), but it can proved that the two definitions are naturally equivalent.

(2) The functor we have just defined depends on the geometric point $x : \mathrm{Spec}(\Omega) \to X$. However, if X is connected, the functors obtained considering two different geometric points of X are isomorphic. This is a consequence of theorem 1.4.34(c), together with the theorem 2.3.10, which we are about to prove.

Theorem 2.3.10. *Let X be a connected scheme and let $x : \mathrm{Spec}(\Omega) \to X$ be a geometric point of X (we know that such a point exists by remark 2.3.2). Let F_x : $\mathbf{FEt}_X \to \mathbf{sets}$ be the functor defined in lemma 2.3.8. Then $\mathbf{FEt}_X$ is an essentially small Galois category with fundamental functor F_x.*

Proof. We omit the proof that $\mathbf{FEt}_X$ is essentially small. We check now that the conditions listed in definition 1.1.4 are satisfied (the proof of the axioms (G4)-(G6) is just sketched).

(G1) Consider $\mathrm{id}_X : X \to X$. We have that id_X is totally split (example 2.2.36) and so it is finite étale by lemma 2.2.37. For any finite étale covering $f : Y \to X$, we have that f is a morphism of schemes with $f = \mathrm{id}_X \circ f$, so f is a morphism of coverings from f to id_X. It is clearly the unique such morphism. This proves that id_X is a terminal object in $\mathbf{FEt}_X$.
The existence of fibred products was proved in lemma 2.2.54.

(G2) Let $(f_i : Y_i \to X)_{i\in I}$ be a finite collection of finite étale coverings of X. We can clearly assume $I = \{1, \dots, n\}$ for some $n \in \mathbb{N}$. Define $Y := \coprod_{i=1}^{n} Y_i$ and let $f : Y \to X$ be the morphism of schemes obtained by gluing the f_i's. By lemma 2.2.18(3), we have that f is a finite étale covering of X. For any $i = 1, \dots, n$ denote by $q_i : Y_i \to Y$ the canonical inclusion, which is a morphism of schemes. Then, by definition of f, for any $i = 1, \dots, n$ we have that $f \circ q_i = f_i$, i.e q_i is a morphism of coverings from f_i to f. Let now Z be a scheme, $g : Z \to X$ a finite étale covering of X and $h_i : Y_i \to Z$ a morphism of coverings from f_i to g (i.e. h_i is a morphism of schemes and $f_i = g \circ h_i$) for any $i = 1, \dots, n$. We can glue the morphisms h_i's and get a unique morphism of schemes $h : Y \to Z$ such that $h \circ q_i = h_i$ for any $i = 1, \dots, n$. Then, for any $i = 1, \dots, n$, we have that $g \circ h \circ q_i = g \circ h_i = f_i = f \circ q_i$, i.e. $(g \circ h)_{|Y_i} = f_{|Y_i}$. Since the Y_i's cover Y, this implies that $g \circ h = f$. So h is a morphism of coverings from f to g. Hence $f : Y \to X$ is the sum of the f_i's in $\mathbf{FEt}_X$.
Fot the existence of quotients by finite groups of automorphisms, see 2.2.57 and the above discussion.

(G3) Let $f : Y \to X$, $g : Z \to X$ be finite étale coverings of X and let $h : Y \to Z$ be a morphism of coverings from f to g. By lemma 2.2.51, h is finite étale. Then, by corollary 2.2.26, we have that $\mathrm{Im}(h) = \{z \in \mathrm{sp}(Z) \mid [Y : Z](y) \geq 1\}$ is both open and closed in Z. Define $Z' := Z \setminus \mathrm{Im}(h)$. Then $\mathrm{Im}(h)$ and Z' are both open subschemes of Z and $Z = \mathrm{Im}(h) \amalg Z'$. Consider the restrictions $g'' := g_{|h(Y)} : h(Y) \to X$ and $g' := g_{|Y'} : Y' \to X$. Since g is finite étale, by lemma 2.2.18(3) we have that g' and g'' are also finite étale. Define $u'' := h : Y \to h(Y)$ and let $u' : h(Y) \to Z$ be the canonical inclusion. Then u' and u'' are morphism of schemes. We have that $g'' = g_{|h(Y)} = g \circ u'$, so u' is a morphism of coverings from g'' to g. Moreover, $g'' \circ u'' = g_{|h(Y)} \circ h = g \circ h = f$ (because h is a morphism of coverings from f to g) and so u'' is a morphism of coverings from f to g''. Clearly $h = u' \circ u''$. Moreover, u'' is surjective by definition. By lemma 2.2.53, this implies that u'' is an epimorphism in $\mathbf{FEt}_X$. We have that $u' : h(Y) \to u'(h(Y)) = h(Y)$ is the identity, in particular it is

an isomorphism of schemes. Then, by lemma 2.2.56, u' is a monomorphism in $\mathbf{FEt}_X$.
Assume now that h is a monomorphism in $\mathbf{FEt}_X$. As above, $Z = \mathrm{Im}(h) \amalg Z'$ and $g' = g_{|_{Z'}}$, $g'' = g_{|_{h(Y)}}$ are finite étale coverings of X. By lemma 2.2.56, we have that $h : Y \to h(Y)$ is an isomorphism of schemes. Moreover, $g' \circ h = g_{|_{Z'}} \circ h = g \circ h = f$, so $h : Y \to h(Y)$ is a morphism of coverings from f to g'. Consider the inverse $h^{-1} : h(Y) \to Y$. Since $g' \circ h = f$, we have that $g' = f \circ h^{-1}$, so h^{-1} is a morphism of coverings from g' to f. This proves that h is an isomorphism from f to g' in $\mathbf{FEt}_X$. Moreover g, together with the canonical inclusions $\mathrm{Im}(h) \to Z$ and $Z' \to Z$ is the sum of g'' and g' in $\mathbf{FEt}_X$, as in the proof of (G2).

(G4) It follows almost immediately from the proof of (G1) and from example 1.1.3(1)-(2).

(G5) The fact that F_x commutes with finite sums follows from the proof of (G2) and from example 1.1.3(3). In order to show that F_x transforms epimorphisms in epimorphisms of finite sets (i.e. surjective functions, see example 1.1.3(6)), one can prove that this holds if $X = \mathrm{Spec}(\Omega)$ and $x = \mathrm{id}_{\mathrm{Spec}(\Omega)}$ and then use lemma 2.2.28(3). Finally, the fact that F_x commutes with quotients by finite groups of automorphisms can be proved using lemma 2.2.58, together with example 1.1.3(5).

(G6) Let $f : Y \to X$, $g : Z \to X$ be finite étale coverings of X and $h : Y \to Z$ a morphism of coverings such that $F_x(h) : F_x(f) \to F_x(g)$ is an isomorphism in **sets**, i.e. a bijection. Then $|F_x(f)| = |F_x(g)|$. Since X is connected, we have that $[Y : X]$ and $[Z : X]$ are constant. Then, by lemma 2.3.7, we have that $[Y : X] = |F_x(f)| = |F_x(g)| = [Z : X]$. By lemma 2.2.51 we have that h is finite étale. Then, by corollary 2.2.26, we have that $h(Y)$ is both open and closed in Z and so we can write $Z = h(Y) \amalg Z'$, where $Z' := Z \backslash h(Y)$. Let $g' = g_{|_{Z'}} : Z' \to X$ and $g'' = g_{|_{h(Y)}} : h(Y) \to X$. As in the proof of (G3), we have that g' and g'' are finite étale coverings of X and g is the sum of g'' and g'. Using the fact that F_x commutes with finite sums, one shows that h is surjective. The surjectivity of h, together with the fact that $[Y : X] = [Z : X]$, implies that h is an isomorphism of schemes (this can be proved firstly in the case when f and g are totally split, using lemma 2.2.48, and then generalized using proposition 2.2.43). Then h is an isomorphism in $\mathbf{FEt}_X$.

□

Remark 2.3.11. In the proof of theorem 2.3.10, the only point where we applied that X is connected was (G6).

Corollary 2.3.12 (Main theorem of Galois theory for schemes)**.** *Let X be a connected scheme. Then there exists a profinite group $\pi(X)$, uniquely determined up to isomorphism, such that* $\mathbf{FEt}_X$ *is equivalent to* $\pi(X)$**-sets**. *Moreover, $\pi(X)$ is isomorphic to* $\mathrm{Aut}(F_x)$ *for any geometric point* $x : \mathrm{Spec}(\Omega) \to X$*, where* $F_x : \mathbf{FEt}_X \to$ **sets** *is defined as in*

Proof. It follows immediately from the theorem 2.3.10 and from the main theorem about Galois categories (1.4.34). □

Definition 2.3.13. Let X is a connected scheme and $x : \mathrm{Spec}(\Omega) \to X$ a geometric point of X. We define $\pi(X, x) := \mathrm{Aut}(F_x)$ the *étale fundamental group of X in x*, where $F_x : \mathbf{FEt}_X \to \mathbf{sets}$ is the functor defined in lemma 2.3.8.

Remark 2.3.14. The fundamental group defined as in 2.3.13 is functorial in (X, x). More precisely, we can consider the category $\mathbf{Sch}_\bullet$ whose objects are pairs of the form (X, x), with X a connected scheme and $x : \mathrm{Spec}(\Omega) \to X$ a geometric point of X (*base point*), and morphisms are morphisms of schemes that preserve the base points (i.e., a morphism from (X, x) to (Y, y) is a morphism of schemes from $f : X \to Y$ such that $f \circ x = y$). To any object (X, x) of $\mathbf{Sch}_\bullet$ we can associate the Galois category $\mathbf{FEt}_X$ with fundamental functor $F_x : \mathbf{FEt}_X \to \mathbf{sets}$. For any morphism $f : (X, x) \to (Y, y)$ in $\mathbf{Sch}_\bullet$, we can define $G_f : \mathbf{FEt}_Y \to \mathbf{FEt}_X$ via $G_f(g) = p_2 : Z \times_X Y \to Y$ for any finite étale covering $f : Z \to X$ (the fact that p_2 is a finite étale coverings of X follows from lemma 2.2.28(4)), extending it to morphisms in the obvious way. Then it can be proved that the assumptions of lemma 1.4.36 are satisfied and so $\hat{\pi}$ can be extended to a functor $\mathbf{Sch}_\bullet \to \mathbf{Prof}$.

Appendix: finite coverings of topological spaces

In this appendix, we will deal with another example of Galois category: the category of finite coverings of a connected topological space (we do *not* consider the empty space as a connected space). In the first section (based on [1], 3.7-3.10) we will define this category and prove that it satisfies all the axioms introduced in the definition 1.1.4. In the second section, we will compute the fundamental group of a very simple connected topological space (exercise 1.25 in [1]). The cross-references that are internal to the appendix can be distinguished from the ones that come from the rest of the thesis because the latter are identified by three numbers (the first two indicating the chapter and the section, respectively), while the former present only two numbers (the first one indicating the section).

1 A Galois category

We start by recalling the definition.

Definition 1.1. Let X, Y be topological spaces and $f : Y \to X$ a continuous map. We say that f is a *trivial covering* of X if there exist a discrete topological space E and a homeomorphism $\varphi : Y \to X \times E$ such that $f = p_X \circ \varphi$, where $p_X : X \times E \to X$ is the projection on the first coordinate. This is illustrated by the following commutative diagram.

$$\begin{array}{ccc} Y & \xrightarrow{\varphi} & X \times E \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle p_X} & \\ & X & \end{array}$$

We say that f is a *covering* of X if for every $x \in X$ there exists an open subset $U \subseteq X$ such that $x \in U$ and the restriction $f : f^{-1}(U) \to U$ is a trivial covering. A covering $f : Y \to X$ is said to be *finite* if for every $x \in X$ the preimage $f^{-1}(\{x\}) \subseteq Y$ is a finite set. In this case, for any $x \in X$ we call $|f^{-1}(\{x\})|$ the *degree* of f at x.
If X, Y, Z are topological spaces and $f : Y \to X$, $g : Z \to X$ are coverings of X, then a *morphism of coverings* from f to g is a continuous map $h : Y \to Z$ such that $g \circ h = f$.

Remark 1.2. (1) Let X be a topological space. It is immediate to check that the composition of two morphisms of coverings is again a morphism of coverings.

Moreover, for any covering $f : Y \to X$ we have that id_Y is clearly a morphism of coverings from f to f. This shows that coverings of X form a category. We will restrict our attention to *finite* coverings. We denote the category of finite coverings of X by $\mathbf{Cov}_X$.

(2) Let X, Y be topological spaces and $f : Y \to X$ a finite covering of X. The map

$$d : X \to \mathbb{N},\ x \mapsto |f^{-1}(\{x\})|$$

is continuous, if we consider the discrete topology on $\mathbb{N}$. Indeed, if $n \in \mathbb{N}$, let $x \in d^{-1}(\{n\})$, i.e. $|f^{-1}(\{x\})| = n$. By definition of covering, there exists an open subset $U \subseteq X$ such that $x \in U$ and $f : f^{-1}(U) \to U$ is a trivial covering. So there exist a discrete topological space E and a homeorphism $\varphi : f^{-1}(U) \to U \times E$ such that $f = p_U \circ \varphi$, where $p_U : U \times E \to U$ is the projection on the first coordinate. For any $x' \in U$, we have that $f^{-1}(\{x'\}) = (p_U \circ \varphi)^{-1}(\{x'\}) = \varphi^{-1}(p_U^{-1}(\{x'\})) = \varphi^{-1}(\{x'\} \times E)$. Since φ is a homeomorphism, it is bijective, so we have $|f^{-1}(\{x'\})| = |\varphi^{-1}(\{x'\} \times E)| = |\{x'\} \times E| = |E|$. Since $x \in U$, this holds in particular for x, so $n = |f^{-1}(\{x\})| = |E| = |f^{-1}(\{x'\})|$ for any $x' \in U$. This shows that $U \subseteq d^{-1}(\{n\})$. Hence $d^{-1}(\{n\})$ is open, which shows that d is continuous.
In particular, if X is connected we have that d is a constant map, i.e. f has the same degree at all points of X. We call this degree the *degree of f*.

Our aim in this section is to prove that, if X is a connected topological space, then $\mathbf{Cov}_X$ is an essentially small Galois category. First of all we have to define a functor $\mathbf{Cov}_X \to \mathbf{sets}$.

Lemma 1.3. *Let $X \neq \emptyset$ be a topological space and fix $x \in X$. For any finite covering $f : Y \to X$, define $F_x(f) = f^{-1}(\{x\})$. Moreover, if $f : Y \to X$ and $g : Z \to X$ are finite coverings of X and $h : Y \to Z$ is a morphism of coverings, we define*

$$F_x(h) : F_x(f) = f^{-1}(\{x\}) \to F_x(g) = g^{-1}(\{x\}),\ y \mapsto h(y)\ .$$

Then $F_x : \mathbf{Cov}_X \to \mathbf{sets}$ is a functor.

Proof. First of all, if $f : Y \to X$ is a finite covering, then $f^{-1}(\{x\})$ is a finite set. So it is indeed an object of **sets**.
Let $f : Y \to X$ and $g : Z \to X$ be finite coverings of X and $h : Y \to Z$ a morphism of coverings. We have to show that $F_x(h)$ is a well-defined map. Let $y \in f^{-1}(\{x\})$. Then and $f(y) = x$. Since h is a morphism of coverings, we have that $f = g \circ h$. Then $x = f(y) = g(h(y))$. So $h(y) \in g^{-1}(\{x\})$ and this shows that $F_x(h) : F_x(f) \to F_x(g)$ is well defined.
Let $f : Y \to X$ be a finite covering and $h = \mathrm{id}_Y$. Then, for any $y \in F_x(f) = f^{-1}(\{x\})$, we have $F_x(h)(y) = h(y) = \mathrm{id}_Y(y) = y$. So $F_x(h) = \mathrm{id}_{F_x(f)}$. Let now $f_1 : Y \to X$, $f_2 : Z \to X$, $f_3 : W \to X$ be finite coverings of X and let $h_1 : Y \to Z$, $h_2 : Z \to W$ be morphisms of coverings. For any $y \in F_x(f) = f_1^{-1}(\{x\})$, we have

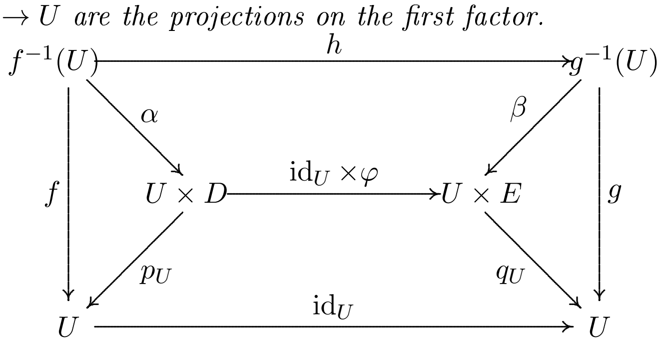
$$\begin{aligned} F_x(h_2 \circ h_1)(y) &= (h_2 \circ h_1)(y) = h_2(h_1(y)) = \\ &= h_2(F_x(h_1)(y)) = F_x(h_2)(F_x(h_1)(y)) = (F_x(h_2) \circ F_x(h_1))(y)\ . \end{aligned}$$

So $F_x(h_2 \circ h_1) = F_x(h_2) \circ F_x(h_1)$. Hence F_x is a functor. □

Remark 1.4. The functor we defined in 1.3 depends on the point x we fixed. However, if X is connected, the functors obtained considering two different points of X are isomorphic. This could be proved directly, but is also a consequence of theorem 1.4.34(c), together with the proposition 1.8 of this appendix, whose proof is now our main concern.

The key tool in the proof of the fact that, if X is a connected topological space, $\mathbf{Cov}_X$ is a Galois category with fundamental functor F_x (for a fixed $x \in X$) will be the following lemma, which says that not only is each finite covering locally trivial, but also morphisms between finite coverings are "locally trivial", in the sense that we will explain.

Lemma 1.5. *Let X, Y, Z be topological spaces, $f : Y \to X$ and $g : Z \to X$ finite coverings and $h : Y \to Z$ a morphism of coverings between f and g. For any $x \in X$, there exists an open neighbourhood U of x in X such that f, g and h are "trivial above U", i.e. such that there exist finite discrete topological spaces D and E, homeomorphisms $\alpha : f^{-1}(U) \to U \times D$ and $\beta : g^{-1}(U) \to U \times E$ and a map $\varphi : D \to E$ such that the following diagram is commutative, where $p_U : U \times D \to U$ and $q_U : U \times E \to U$ are the projections on the first factor.*



Proof. Let $x \in X$. By definition of covering, there exist open neighbourhoods V_1, V_2 of x in X such that $f : f^{-1}(V_1) \to V_1$ and $g : g^{-1}(V_2) \to V_2$ are trivial coverings. This means that there exist discrete topological spaces D and E and homeomorphisms $\alpha : f^{-1}(V_1) \to V_1 \times D$, $\beta : g^{-1}(V_2) \to V_2 \times E$ such that $p_{V_1} \circ \alpha = f$ and $q_{V_2} \circ \beta = g$, where $p_{V_1} : V_1 \times D \to V_1$ and $q_{V_2} : V_2 \times E \to V_2$ are the projections on the first factor. Since the coverings are finite, D and E are finite. Define $V := V_1 \cap V_2$. Then also V is an open neighbourhood of x in X. Notice that $f^{-1}(V) = (p_{V_1} \circ \alpha)^{-1}(V) = \alpha^{-1}(p_V^{-1}(V)) = \alpha^{-1}(V \times D)$. So $\alpha(fi^{-1}(V)) = V \times D$ and, restricting α to $f^{-1}(V)$, we get a homeomorphism $\alpha : f^{-1}(V) \to V \times D$. Analogously, restricting β to $g^{-1}(V)$, we get a homeomorphism $\beta : g^{-1}(V) \to V \times E$. Clearly, $p_V \circ \alpha = f$ and $q_V \circ \beta = g$, where $p_V : V \times D \to V$ and $q_V : V \times E \to V$ are the projections on the first factor. By definition of morphisms of coverings, $g \circ h = f$. Then, for any $y \in f^{-1}(V)$, we have that $g(h(y)) = f(y) \in V$ and so $h(y) \in g^{-1}(V)$. Then, restricting h to $f^{-1}(V)$, we get a continuous map $h : f^{-1}(V) \to g^{-1}(V)$. Consider the map $\beta \circ h \circ \alpha^{-1} : V \times D \to V \times E$, which is continuous because it is the composition of continuous maps. We have that $q_V \circ \beta \circ h \circ \alpha^{-1} = g \circ h \circ \alpha^{-1} = f \circ \alpha^{-1} = p_V$. Then, for any $(v, d) \in V \times D$, we have

$$\left(\beta \circ h \circ \alpha^{-1}\right)((v, d)) = \left(q_V\left(\left(\beta \circ h \circ \alpha^{-1}\right)((v, d))\right), q_E\left(\left(\beta \circ h \circ \alpha^{-1}\right)((v, d))\right)\right) =$$

$$= (p_V((v,d)), \varphi_v(d)) = (v, \varphi_v(d)) \ ,$$

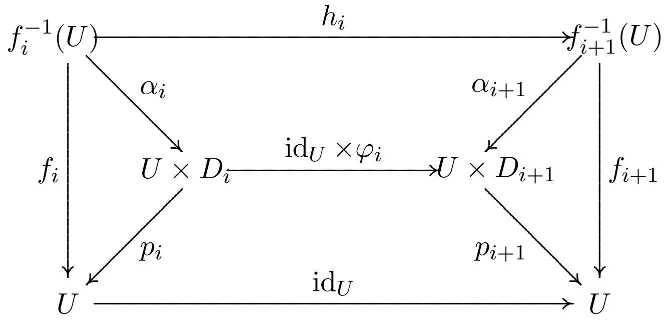
where $q_E : V \times E \to E$ is the projection on the second factor and we defined $\varphi_v : D \to E,\ d \mapsto (q_E \circ \beta \circ h \circ \alpha^{-1})((v,d))$, for any $v \in V$. Define $\varphi := \varphi_x : D \to E$. Then φ is continuous, because we have the discrete topology on D. So the composition $\varphi \circ p_E$ is also continuous, where $p_E : V \times E \to E$ is the projection on the second factor. Consider the map

$$\gamma : V \times D \to E \times E,\ (v,d) \mapsto (\varphi(d), \varphi_v(d)) \ .$$

We have that γ is continuous, because its components are $\varphi \circ p_E$ and $q_V \circ \beta \circ h \circ \alpha^{-1}$, which are continuous. Since E has the discrete topology, the product $E \times E$ is also discrete. Then the diagonal $\Delta := \{(e,e) \mid e \in E\} \subseteq E \times E$ is open in $E \times E$. It follows that $\gamma^{-1}(\Delta)$ is open in $V \times D$. It is clear, from the definitions of γ and of φ, that $\{x\} \times D \subseteq \gamma^{-1}(\Delta)$. Then, applying the definition of product topology, we get that for any $d \in D$ there exists an open neighbourhood U_d of x in V such that $U_d \times \{d\} \subseteq \gamma^{-1}(\Delta)$ (notice that, since V is open in X, U_d is open also in X). Define $U := \bigcap_{d \in D} U_d$. Then U is an open neighbourhood of x, because it is a finite intersection of open neighbourhoods of x (remember that D is finite). Let $(u,d) \in U \times D$. Since $U \subseteq U_d$, we have that $(u,d) \in U_d \times \{d\} \subseteq \gamma^{-1}(\Delta)$. So $(\varphi(d), \varphi_u(d)) = \gamma((u,d)) \in \Delta$, which means that $\varphi_u(d) = \varphi(d)$. This shows that $\varphi_u = \varphi$ for any $u \in U$. As above, using the fact that $p_V \circ \alpha = f$ and $q_V \circ \beta = g$, we get that $\alpha(f^{-1}(U)) = U \times D$ and $\beta(g^{-1}(U)) = U \times E$. So, restricting α and β, we get homeomorphisms $\alpha : f^{-1}(U) \to U \times D$ and $\beta : g^{-1}(U) \to U \times E$ such that $p_U \circ \alpha = f$ and $q_U \circ \beta = g$. For any $(u,d) \in U \times D$, we have that $(\beta \circ h \circ \alpha^{-1})((u,d)) = (u, \varphi_u(d)) = (u, \varphi(d))$. So $\beta \circ h \circ \alpha^{-1} = \mathrm{id}_U \times \varphi$. The fact that $q_U \circ (\mathrm{id}_U \times \varphi) = p_U = \mathrm{id}_U \circ p_U$ is obvious. So the diagram is commutative. □

The lemma we have just proved can be generalized to a finite number of morphisms as follows.

Corollary 1.6. *Let $X, Y_1, \dots, Y_n$ be topological spaces ($n \in \mathbb{N}$), $f_1 : Y_1 \to X, \dots, f_n : Y_n \to X$ finite coverings of X and $h_1 : Y_1 \to Y_2, \dots, h_{n-1} : Y_{n-1} \to Y_n$ morphisms of coverings. For any $x \in X$, there exists an open neighbourhood U of x in X such that $f_1, \dots, f_n$, $h_1, \dots, h_{n-1}$ are all trivial above U, in the same sense as in the lemma 1.5: there exist finite discrete topological spaces $D_1, \dots, D_n$, homeomorphisms $\alpha_1 : f_1^{-1}(U) \to U \times D_1, \dots, \alpha_n : f_n^{-1}(U) \to U \times D_n$ and maps $\varphi_1 : D_1 \to D_2, \dots, \varphi_{n-1} : D_{n-1} \to D_n$ such that the following diagram is commutative for any $i = 1, \dots, n-1$, where $p_1 : U \times D_1 \to U, \dots, p_n : U \times D_n \to U$ are the projections on the first factor.*



Proof. By lemma 1.5, for any $i = 1, \dots, n-1$ there exists an open neighbourhood U_i of x in X such that f_i, f_{i+1} and h_i are trivial above U_i. Define $U := \bigcap_{i=1}^{n-1} U_i$. Then U is open in X, because it is a finite intersection of open subsets. Moreover, $x \in U$. So U is an open neighbourhood of x in X. Since $U \subseteq U_i$ for any $i = 1, \dots, n-1$, it is immediate to check that $f_1, \dots, f_n$, $h_1, \dots, h_{n-1}$ are all trivial above U. □

Lemma 1.7. *Let X be a topological space, $f : Y \to X$ and $g : Z \to X$ finite coverings and $h : Y \to Z$ a morphism of coverings from f to g. Then:*

(1) $\mathrm{Im}(h)$ *is both open and closed in Z;*

(2) h is an epimorphism in $\mathbf{Cov}_X$ if and only if it is surjective.

Proof. (1) Let $z \in Z$. Consider $x := g(z)$. By lemma 1.5, there exists an open neighbourhood U of x in X such that f, g and h are trivial above U. This means that there exist finite discrete topological spaces D and E, homeomorphisms $\alpha : f^{-1}(U) \to U \times D$ and $\beta : g^{-1}(U) \to U \times E$ and a map $\varphi : D \to E$ such that $\beta \circ h = (\mathrm{id}_U \times \varphi) \circ \alpha$, $f = p_U \circ \alpha$ and $g = q_U \circ \beta$, where $p_U : U \times D \to U$, $q_U : U \times E \to E$ are the projections on the first factor. Since $g(z) = x \in U$, we have that $z \in g^{-1}(U)$.
Assume that $z \in \mathrm{Im}(h)$. Then there exists $y \in Y$ such that $z = h(y)$. Since h is a morphism of coverings, we have that $f = h \circ g$. So $f(y) = g(h(y)) = g(z) = x \in U$, which implies that $y \in f^{-1}(U)$. Consider $\alpha(y) \in U \times D$. Since $f = p_U \circ \alpha$, we have that $\alpha(y) = (f(y), d) = (x, d)$, for some $d \in D$. Define $e := \varphi(d) \in D$. Let $x' \in U$. Then $(x', d) \in U \times D$ and, since $\beta \circ h \circ \alpha^{-1} = \mathrm{id}_U \times \varphi$, we have that

$$(x', e) = (\mathrm{id}_U \times \varphi)((x', d)) = \beta(h(\alpha^{-1}((x', d)))) \ .$$

So $(x', e) \in \beta(\mathrm{Im}(h))$. This shows that $U \times \{e\} \subseteq \beta(\mathrm{Im}(h))$. Then, since β is a homeomorphism, we have that $\beta^{-1}(U \times \{e\}) \subseteq \mathrm{Im}(h)$. But $U \times \{e\}$ is open in $U \times E$, because E has the discrete topology. So $\beta^{-1}(U \times \{e\})$ is open in $g^{-1}(U)$. Since $g^{-1}(U)$ is open in Z, this implies that $\beta^{-1}(U \times \{e\})$ is open in Z. Moreover, $\beta(z) = \beta(h(y)) = (\mathrm{id}_U \times \varphi)(\alpha(y)) = (\mathrm{id}_U \times \varphi)((x, d)) = (x, \varphi(d)) = (x, e) \in U \times \{e\}$. So $z \in \beta^{-1}(U \times \{e\})$. This shows that $\mathrm{Im}(h)$ is open.
On the other hand, assume that $z \notin \mathrm{Im}(h)$. Consider $\beta(z) \in U \times E$. Since $g = q_U \circ \beta$, we have that $\beta(z) = (g(z), e) = (x, e)$, for some $e \in E$. Let $z' \in \beta^{-1}(U \times \{e\}) \subseteq g^{-1}(U)$ and assume by contradiction that $z' \in \mathrm{Im}(h)$. Then there exists $y \in Y$ such that $z' = h(y)$. Since $f = g \circ h$, we have that $f(y) = g(h(y)) = g(z') \in U$. Then $y \in f^{-1}(U)$. Consider $\alpha(y) \in U \times D$. Since $f = p_U \circ \alpha$, we have that $\alpha(y) = (f(y), d) = (x', d)$, for some $d \in D$, where we defined $x' := f(y) = g(z') \in U$. Moreover, since $z' \in \beta^{-1}(U \times \{e\}) \subseteq g^{-1}(U)$ and $g = q_U \circ \beta$, we have that $\beta(z') = (g(z'), e) = (x', e)$. Then, since $\beta \circ h = (\mathrm{id}_U \times \varphi) \circ \alpha$, we have

$$(x', e) = \beta(z') = \beta(h(y)) = (\mathrm{id}_U \times \varphi)(\alpha(y)) = (\mathrm{id}_U \times \varphi)((x', d)) = (x', \varphi(d)) \ .$$

So $e = \varphi(d)$. Now we have that

$$\beta(z) = (x, e) = (x, \varphi(d)) = (\mathrm{id}_U \times \varphi)((x, d)) = \\ = ((\mathrm{id}_U \times \varphi) \circ \alpha)(\alpha^{-1}((x, d))) = \beta(h(\alpha^{-1}((x, d)))) \ ,$$

which, since β is a homeomorphism, implies that $z = h(\alpha^{-1}((x, d))) \in \mathrm{Im}(h)$. This is a contradiction. So $z' \notin \mathrm{Im}(h)$. This shows that $\beta^{-1}(U \times \{e\}) \subseteq Z \backslash \mathrm{Im}(h)$. But $U \times \{e\}$ is open in $U \times E$, because E has the discrete topology. So $\beta^{-1}(U \times \{e\})$ is open in $g^{-1}(U)$. Since $g^{-1}(U)$ is open in Z, this implies that $\beta^{-1}(U \times \{e\})$ is open in Z. Moreover, $z \in \beta^{-1}(U \times \{e\})$ (because $\beta(z) = (x, e) \in U \times \{e\}$). This shows that $Z \backslash \mathrm{Im}(h)$ is open. Hence $\mathrm{Im}(h)$ is closed.

(2) Assume that h is surjective. By example 1.1.3(6), we have that h is an epimorphism of sets (notice that in the proof we did not use the fact that the sets were finite, so it works for arbitrary sets). Let W be a topological space and $m : W \to X$ a finite covering. Let $l_1, l_2 : Y \to W$ be two morphisms of coverings such that $l_1 \circ h = l_2 \circ h$. In particular, l_1, l_2 are maps between sets. Since h is an epimorphism of sets, this implies that $l_1 = l_2$.
Conversely, assume that h is an epimorphism. Consider the set $E := \{a, b\}$ (with $a \neq b$), endowed with the discrete topology, and the finite trivial covering $p_X : X \times E \to X$ (projection on the first factor). Define

$$l_1 : Z \to X \times E, \ z \mapsto (g(z), a)$$

and

$$l_2 : Z \to X \times E, \ z \mapsto \begin{cases} (g(z), a) & \text{if } z \in \mathrm{Im}(h) \\ (g(z), b) & \text{if } z \notin \mathrm{Im}(h) \end{cases} .$$

It is clear that l_1 is continuous, because its components are g, which is continuous by assumption, and the map $Z \to E, \ z \mapsto a$, which is continuous because it is constant. Let us prove that l_2 is continuous. The first component is g, which is continuous. The second component is

$$m : Z \to E, \ z \mapsto \begin{cases} a & \text{if } z \in \mathrm{Im}(h) \\ b & \text{if } z \notin \mathrm{Im}(h) \end{cases} .$$

We have that $m^{-1}(\{a\}) = \mathrm{Im}(h)$ and $m^{-1}(\{b\}) = Z \backslash \mathrm{Im}(h)$. Both are open, by point (1). So l_2 is continuous. From the definitions of l_1 and l_2, it is clear that $p_X \circ l_1 = g = p_X \circ l_2$. This means that l_1 and l_2 are morphisms of coverings. For any $y \in Y$, we have that $h(y) \in \mathrm{Im}(h)$ and so $l_2(h(y)) = (g(h(y)), a) = l_1(h(y))$. So $l_1 \circ h = l_2 \circ h$. Since h is an epimorphism, this implies that $l_1 = l_2$. Then, for any $z \in Z$, we have that $l_2(z) = l_1(z) = (g(z), a)$, which implies that $z \in \mathrm{Im}(h)$. Hence h is surjective.

□

Proposition 1.8. *Let X be a connected topological space (in particular, $X \neq \emptyset$) and fix $x \in X$. Let $F_x : \mathbf{Cov}_X \to \mathbf{sets}$ be the functor defined in lemma 1.3. Then $\mathbf{Cov}_X$ is an essentially small Galois category with fundamental functor F_x.*

Proof. First of all, we prove that $\mathbf{Cov}_X$ is essentially small. It is enough to show that, for any $n \in \mathbb{N}$, the collection of isomorphism classes of coverings of X of degree n (see remark 1.2(2)) is a set. If $f : Y \to X$ is a covering of degree n, then there is a bijection $\varphi : Y \to X \times \{1, \dots, n\}$ such that $f = p_X \circ \varphi$, where $p_X : X \times \{1, \dots, n\} \to X$ is the projection on the first factor. Then φ induces a topology on $X \times \{1, \dots, n\}$ such that φ becomes a homeomorphism (notice that, if we consider the product topology on $X \times \{1, \dots, n\}$, then φ is in general only a bijection, not a homeomorphism: if it is a homeomorphism, then f is a trivial covering). Then f is isomorphic to p_X. The collection of all possible topologies on $X \times \{1, \dots, n\}$ is a set, because it is a subset of the power set of the power set of X. Then the collection of isomorphism classes of coverings of X of degree n is a set. Hence $\mathbf{Cov}_X$ is essentially small.
We check now that the conditions listed in definition 1.1.4 are satisfied.

(G1) Consider the map $\mathrm{id}_X : X \to X$ (which is clearly continuous). We have an obvious homeomorphism $\varphi : X \to X \times \{1\}$, $x \mapsto (x, 1)$ and clearly $p_X \circ \varphi = \mathrm{id}_X$ (where $p_X : X \times \{1\} \to X$ is the projection on the first factor). So id_X is a trivial finite covering. For any finite covering $f : Y \to X$, we have that f is continuous and $\mathrm{id}_X \circ f = f$, so f is a morphism of coverings from f to id_X. It is clearly the unique such morphism. This proves that id_X is a terminal object in $\mathbf{Cov}_X$.
Let $f_1 : Y_1 \to X$, $f_2 : Y_2 \to X$, $g : Z \to X$ be finite coverings, $h_1 : Y_1 \to Z$ and $h_2 : Y_2 \to Z$ two morphisms of coverings. This means that $g \circ h_1 = f_1$ and $g \circ h_2 = f_2$. Consider the fibred product $Y_1 \times_Z Y_2$ as defined in example 1.1.3(2), with the subspace topology of the product. Let $p_1 : Y_1 \times_Z Y_2 \to Y_1$, $p_2 : Y_1 \times_Z Y_2 \to Y_2$ be the projections, which are continuous by definition of the product topology, and define $f := f_1 \circ p_1 : Y_1 \times_Z Y_2 \to X$. Then f is continuous, because it is the composition of continuous functions. Notice that $f = f_1 \circ p_1 = g \circ h_1 \circ \circ p_1 = g \circ h_2 \circ p_2 = f_2 \circ p_2$, since $h_1 \circ p_1 = h_2 \circ p_2$ by definition of the fibred product of sets. We claim that f is a finite covering of X. Let $x' \in X$. By corollary 1.6, there exists an open neighbourhooud U of x' in X such that f_1, f_2, g, h_1, h_2 are all trivial above U. This means that we have finite discrete topological spaces D_1, D_2 and E, homeomorphisms $\alpha_1 : f_1^{-1}(U) \to U \times D_1$, $\alpha_2 : f_2^{-1}(U) \to U \times D_2$ and $\beta : g^{-1}(U) \to U \times E$ and two maps $\varphi_1 : D_1 \times E$, $\varphi_2 : D_2 \times E$ such that: $\beta \circ h_1 = (\mathrm{id}_U \times \varphi_1) \circ \alpha_1$, $\beta \circ h_2 = (\mathrm{id}_U \times \varphi_2) \circ \alpha_2$, $r_1 \circ \alpha_1 = f_1$, $r_2 \circ \alpha_2 = f_2$ and $q \circ \beta = g$, where $r_1 : U \times D_1 \to U$, $r_2 : U \times D_2 \to D_2$ and $q : U \times E \to E$ are the projections on the first factor. We have that

$$
\begin{aligned}
f^{-1}(U) &= \{(y_1, y_2) \in Y_1 \times_Z Y_2 \mid f((y_1, y_2)) \in U\} = \\
&= \{(y_1, y_2) \in Y_1 \times Y_2 \mid h_1(y_1) = h_2(y_2),\ f_1(y_1) \in U,\ f_2(y_2) \in U\} = \\
&= \{(y_1, y_2) \in f_1^{-1}(U) \times f_2^{-1}(U) \mid h_1(y_1) = h_2(y_2)\} = \\
&= f_1^{-1}(U) \times_Z f_2^{-1}(U) = f_1^{-1}(U) \times_{g^{-1}(U)} f_2^{-1}(U)
\end{aligned}
$$

(the last equality is justified by the fact that $h_1(f_1^{-1}(U)) \subseteq g^{-1}(U)$ and $h_2(f_2^{-1}(U)) \subseteq g^{-1}(U)$). Then the homeomorphisms α_1, α_2 and β induce a homeomorphism

$$\gamma : f^{-1}(U) = f_1^{-1}(U) \times_{g^{-1}(U)} f_2^{-1}(U) \to (U \times D_1) \times_{U \times E} (U \times D_2),$$
$$(y_1, y_2) \mapsto (\alpha_1(y_1), \alpha_2(y_2))$$

(it is straightforward to check that this is a well-defined homeomorphism). We claim that $(U \times D_1) \times_{U \times E} (U \times D_2) \cong U \times (D_1 \times_E D_2)$. Define

$$\vartheta : U \times (D_1 \times_E D_2) \to (U \times D_1) \times_{U \times E} (U \times D_2),\ (u, (d_1, d_2)) \mapsto ((u, d_1), (u, d_2))\ .$$

Let us prove that ϑ is well defined. If $(u, (d_1, d_2)) \in U \times (D_1 \times_E D_2)$, then $\varphi_1(d_1) = \varphi_2(d_2)$. So

$$(\mathrm{id}_U \times \varphi_1)((u, d_1)) = (u, \varphi_1(d_1)) = (u, \varphi_2(d_2)) = (\mathrm{id}_U \times \varphi_2)((u, d_2))$$

and this proves that $((u, d_1), (u, d_2)) \in (U \times D_1) \times_{U \times E} (U \times D_2)$. So ϑ is well defined. We have that ϑ is continuous, because its components are continuous. It is also clear that ϑ is injective. We prove now that it is surjective. Let $((u_1, d_1), (u_2, d_2)) \in (U \times D_1) \times_{U \times E} (U \times D_2)$. This means that $(u_1, \varphi_1(d_1)) = (\mathrm{id}_U \times \varphi_1)((u_1, d_1)) = (\mathrm{id}_U \times \varphi_2)((u_2, d_2)) = (u_2, \varphi_2(d_2))$. So $u_1 = u_2$ and $\varphi_1(d_1) = \varphi_2(d_2)$. Then $(d_1, d_2) \in D_1 \times_E D_2$ and $(u_1, (d_1, d_2)) \in U \times (D_1 \times_E D_2)$. Moreover,

$$\vartheta((u_1, (d_1, d_2))) = ((u_1, d_1), (u_1, d_2)) = ((u_1, d_1), (u_2, d_2))\ .$$

This shows that ϑ is surjective. Finally, the inverse map

$$\vartheta^{-1} : (U \times D_1) \times_{U \times E} (U \times D_2) \to U \times (D_1 \times_E D_2),$$
$$((u_1, d_1), (u_2, d_2)) \mapsto (u_1 = u_2, (d_1, d_2))$$

is also continuous, because its components are continuous. So ϑ is a homeomorphism. Now we have a homeomorphism $\vartheta^{-1} \circ \gamma : f^{-1}(U) \to U \times (D_1 \times_E D_2)$ and $D_1 \times_E D_2$ is a finite discrete topological space. Denote by $p : U \times (D_1 \times_E D_2) \to U$ the projection on the first factor. From the definition of ϑ, it follows that $p \circ \vartheta^{-1} = r_1 \circ s_1$, where $s_1 : (U \times D_1) \times_{U \times E} (U \times D_2) \to U \times D_1$ is the projection on the first factor. On the other hand, from the definition of γ we have that $s_1 \circ \gamma = \alpha_1 \circ p_1$. So $p \circ (\vartheta^{-1} \circ \gamma) = r_1 \circ s_1 \circ \gamma = r_1 \circ \alpha_1 \circ p_1 = f_1 \circ p_1 = f$. This proves that f is a finite covering of X. Since $f = f_1 \circ p_1$, we have that p_1 is a morphism a coverings from f to f_1. Analogously, since $f = f_2 \circ p_2$, we have that p_2 is a morphism of coverings from f to f_2. We have also that $h_1 \circ p_1 = h_2 \circ p_2$, by definition of the fibred product of sets. Let now W be a topological space and $m : W \to X$ a finite covering, with two morphisms of coverings $l_1 : W \to Y_1$, $l_2 : W \to Y_2$, such that $h_1 \circ l_1 = h_2 \circ l_2$. As in example 1.1.3(2), we have a unique map $l : W \to Y_1 \times_Z Y_2$ such that $l_1 = p_1 \circ l$ and $l_2 = p_2 \circ l$. This map is continuous because its components are continuous. Moreover, $f \circ l = f_1 \circ p_1 \circ l = f_1 \circ l_1 = m$, where the last equality follows from the fact that l_1 is a morphism of coverings from m to f_1. This means that l is a morphism of coverings from m to f. Hence $f : Y_1 \times_Z Y_2 \to X$ is the fibred product of $f_1 : Y_1 \to X$ and $f_2 : Y_2 \to X$ over $g : Z \to X$ in the category $\mathbf{Cov}_X$.

(G2) Let $(f_i : Y_i \to X)_{i\in I}$ be a finite collection of finite coverings of X. Let Y be the disjoint union $\coprod_{i\in I} Y_i$, with inclusions $q_j : Y_j \to Y$, for any $j \in I$. Recall that the topology on the disjoint union is defined in such a way that a map from $\coprod_{i\in I} Y_i$ to any topological space is continuous if and only if its restriction to Y_j is continuous for any $j \in I$. Consider now the map

$$f : Y \to X,\ y \mapsto f_j(y)\ ,$$

where j is the unique element of I such that $y \in Y_j$. Then $f \circ q_j = f_j$ for any $j \in I$ and f is continuous by definition of the topology on the disjoint union. We claim that f is a finite covering of X. Let $x' \in X$. For any $j \in I$, since f_j is a finite covering of X, there exists an open neighbourhood U_j of x' in X such that $f_j : f_j^{-1}(U) \to U$ is a trivial finite covering, i.e. there exist a finite discrete topological space E_j and a homeomorphism $\varphi_j : f_j^{-1}(U) \to U \times E_j$ such that $f_j = p_j \circ \varphi_j$, where $p_j : U_j \times E_j \to U_j$ is the projection on the first factor. Define $U := \bigcap_{i\in I} U_i$. Since I is finite, U is an open neighbourhood of x' in X. For any $j \in I$, we have that $f_j^{-1}(U) = (p_j \circ \varphi_j)^{-1}(U) = \varphi_j^{-1}(p_j^{-1}(U)) = \varphi_j^{-1}(U \times E_j)$. So $\varphi_j(f_j^{-1}(U)) = U \times E_j$ and, restricting φ_j to $f_j^{-1}(U)$, we get a homeomorphism $\varphi_j : f_j^{-1}(U) \to U \times E_j$. By definition of f, we have that

$$f^{-1}(U) = \left\{ y \in Y = \coprod_{i\in I} Y_i \;\middle|\; f(y) \in U \right\} = \\ = \coprod_{i\in I} \{ y \in Y_i \mid f_i(y) = f(y) \in U \} = \coprod_{i\in I} f_i^{-1}(U)\ .$$

Define $\varphi : f^{-1}(U) = \coprod_{i\in I} f_i^{-1}(U) \to \coprod_{i\in I} (U \times E_i),\ y \mapsto \varphi_j(y)$, where j is the unique element of I such that $y \in Y_j$. It is straightforward to check that φ is a homeomorphism. Moreover, consider

$$\vartheta : U \times \left(\coprod_{i\in I} E_i \right) \to \coprod_{i\in I} (U \times E_i),\ (u,e) \mapsto (u,e)\ .$$

This is well defined, because if $(u,e) \in U \times \left(\coprod_{i\in I} E_i\right)$ we have that $u \in U$ and there exists a unique $j \in I$ such that $e \in E_j$, so $(u,e) \in U \times E_j \subseteq \coprod_{i\in I}(U \times E_i)$. It is obvious that ϑ is bijective. Moreover, ϑ is continuous. Indeed, a base of open subsets of $\coprod_{i\in I}(U \times E_i)$ is given by

$$\bigcup_{i\in I} \{ V \times \{e\} \mid V \subseteq U \text{ open},\ e \in E_i \}$$

and, for any $j \in I$, $V \subseteq U$ open and $e \in E_j$, we have that $\vartheta^{-1}(V) = V \times \{e\}$ is open in $U \times \left(\coprod_{i\in I} E_i\right)$, because $\coprod_{i\in I} E_i$ has the discrete topology. Also the inverse

$$\vartheta^{-1} : \coprod_{i\in I} (U \times E_i) \to U \times \left(\coprod_{i\in I} E_i \right),\ (u,e) \mapsto (u,e)\ .$$

is continuous, because the restriction to $U \times E_j$ is continuous for any $j \in I$. So ϑ is a homeomorphism. Now we have a homeomorphism $\vartheta^{-1} \circ \varphi : f^{-1}(U) \to U \times \left(\coprod_{i \in I} E_i\right)$ and $\coprod_{i \in I} E_i$ is a finite discrete topological space (because I is finite and E_j is a finite discrete topological space for any $j \in I$). Denote by $p_U : U \times \left(\coprod_{i \in I} E_i\right) \to U$ the projection on the first factor and by $q'_j : U \times E_j \to \coprod_{i \in I}(U \times E_i)$ the canonical inclusion, for any $j \in I$. Let $j \in I$. From the definition of ϑ, it follows that $p_U \circ \vartheta^{-1} \circ q'_j = p_j$. Moreover, from the definition of φ, we have that $\varphi \circ q_j = q'_j \circ \varphi_j$. Then

$$p_U \circ \vartheta^{-1} \circ \varphi \circ q_j = p_U \circ \vartheta^{-1} \circ q'_j \circ \varphi_j = p_j \circ \varphi_j = f_j = f \circ q_j \ .$$

Since this holds for any $j \in I$, we must have $p_U \circ (\vartheta^{-1} \circ \varphi) = f$. So f is a finite covering of X. For any $j \in I$, we have that $q_j : Y_j \to Y$ is a morphism of coverings from f_j to f, because $f \circ q_j = f_j$. Let now Z be a topological space, $g : Z \to X$ a finite covering and $h_j : Y_j \to Z$ a morphism of coverings (i.e. h_j continuous and $g \circ h_j = f_j$), for any $j \in I$. As in example 1.1.3(3), we have a unique $h : Y = \coprod_{i \in I} Y_i \to Z$ such that $h_j = h \circ q_j$ for any $j \in I$. This map is continuous, because for any $j \in I$ its restriction to Y_j is h_j, which is continuous. Moreover, we have that $g \circ h \circ q_j = g \circ h_j = f_j = f \circ q_j$ for any $j \in I$ and this implies that $g \circ h = f$. So h is a morphism of coverings from f to g. Hence $f : Y \to X$ is the sum of the f_i's in $\mathbf{Cov}_X$.
Let now $f : Y \to X$ be a finite covering and G a finite subgroup of $\mathrm{Aut}_{\mathbf{Cov}_X}(f)$. Notice that any automorphism of f is in particular a homeomorphism of Y. Then we can consider the set of orbits Y/G, provided with the quotient topology. For any $\sigma \in G$, we have that $f \circ \sigma = f$, because σ is a morphism of coverings. Then, as in example 1.1.3(5), we can define $\overline{f} : Y/G \to X,\ Gy \mapsto f(y)$ and we have $f = \overline{f} \circ p$, where $p : Y \to Y/G,\ y \mapsto Gy$ is the canonical projection. By definition of quotient topology, $\overline{f}$ is continuous. We claim that $\overline{f}$ is a finite covering of X. Let $x' \in X$. Since G is finite, by corollary 1.6 there exists an open neighbourhood U of x' in X such that f is trivial above U and any $\sigma \in G$ is trivial above U. This means that there exist a finite discrete topological space D, a homeomorphism $\alpha : f^{-1}(U) \to U \times D$ and maps $\varphi_\sigma : D \to D$, for any $\sigma \in G$, such that $f = p_U \circ \alpha$, where $p_U : U \times D \to U$ is the projection on the first factor, and $\alpha \circ \sigma = (\mathrm{id}_U \times \varphi_\sigma) \circ \alpha$, for any $\sigma \in G$. Let $\sigma, \tau \in G$. We have that

$$(\mathrm{id}_U \times \varphi_{\sigma \circ \tau}) \circ \alpha = \alpha \circ \sigma \circ \tau = (\mathrm{id}_U \times \varphi_\sigma) \circ \alpha \circ \tau = (\mathrm{id}_U \times \varphi_\sigma) \circ (\mathrm{id}_U \times \varphi_\tau) \circ \alpha \ .$$

Since α is a homeomorphism, this implies that $\mathrm{id}_U \times \varphi_{\sigma \circ \tau} = (\mathrm{id}_U \times \varphi_\sigma) \circ (\mathrm{id}_U \times \varphi_\tau) = \mathrm{id}_U \times (\varphi_\sigma \circ \varphi_\tau)$. Then $\varphi_{\sigma \circ \tau} = \varphi_\sigma \circ \varphi_\tau$. Since G is a subgroup of $\mathrm{Aut}_{\mathbf{Cov}_X}(f)$, we have that $\mathrm{id}_Y \in G$. Moreover, $(\mathrm{id}_U \times \varphi_{\mathrm{id}_Y}) \circ \alpha = \alpha \circ \mathrm{id}_Y = \alpha = \mathrm{id}_{U \times D} \circ \alpha$. Since α is a homeomorphism, we get that $\mathrm{id}_U \times \varphi_{\mathrm{id}_Y} = \mathrm{id}_{U \times D} = \mathrm{id}_U \times \mathrm{id}_D$ and so $\varphi_{\mathrm{id}_Y} = \mathrm{id}_D$. Since G is a subgroup of $\mathrm{Aut}_{\mathbf{Cov}_X}(f)$, for any $\sigma \in G$ we have that $\sigma^{-1} \in G$. Then, by what we have just proved,

$$\varphi_\sigma \circ \varphi_{\sigma^{-1}} = \varphi_{\sigma \circ \sigma^{-1}} = \varphi_{\mathrm{id}_Y} = \mathrm{id}_D$$

and

$$\varphi_{\sigma^{-1}} \circ \varphi_\sigma = \varphi_{\sigma^{-1} \circ \sigma} = \varphi_{\mathrm{id}_Y} = \mathrm{id}_D \ .$$

So φ_σ is invertible, i.e. φ_σ is in the symmetric group S_D. What we proved above means that the map $\varphi : G \to \mathrm{S}_D$, $\sigma \mapsto \varphi_\sigma$ is a group homomorphism. Then $\mathrm{Im}(\varphi)$ is a subgroup of S_D. Let $\sigma \in G$. If $y \in f^{-1}(U)$, then $f(\sigma(y)) = f(y) \in U$, since $f \circ \sigma = f$. Then $\sigma(y) \in f^{-1}(U)$. So $\sigma(f^{-1}(U)) \subseteq f^{-1}(U)$. On the other hand, since $\sigma^{-1}(y) \in f^{-1}(U)$ by the same argoment, $y = \sigma(\sigma^{-1}(y)) \in \sigma(f^{-1}(U))$. So $\sigma(f^{-1}(U)) = f^{-1}(U)$. This means that, if we restrict σ to $f^{-1}(U)$. we get a homeomorphism $\sigma : f^{-1}(U) \to f^{-1}(U)$. So restriction to $f^{-1}(U)$ maps G to a finite group of automorphisms of the topological space $f^{-1}(U)$. We have that

$$\left(\overline{f}\right)^{-1}(U) = \{Gy \in Y/G \mid f(y) = \overline{f}(y) \in U\} = \\ = \{Gy \in Y/G \mid y \in f^{-1}(U)\} = f^{-1}(U)/G \ .$$

The homeomorphism α induces the following map:

$$\overline{\alpha} : \left(\overline{f}\right)^{-1}(U) = f^{-1}(U)/G \to (U \times D)/(\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi)), \\ Gy \mapsto (\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi))\alpha(y) \ .$$

It is immediate to check that $\overline{\alpha}$ is well defined. Moreover, $\overline{\alpha}$ is continuous by definition of quotient topology, because $\overline{\alpha} \circ p = q \circ \alpha$ is continuous, where $q : U \times D \to (U \times D)/(\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi))$ is the canonical projection. In the same way, the map

$$(U \times D)/(\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi)) \to \left(\overline{f}\right)^{-1}(U) = f^{-1}(U)/G, \\ (\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi))(u, d) \mapsto G\alpha^{-1}((u, d))$$

is well defined and continuous. This map is clearly the inverse of $\overline{\alpha}$, which is then a homeomorphism. Moreover, consider

$$\vartheta : U \times (D/\mathrm{Im}(\varphi)) \to (U \times D)/(\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi)), \\ (u, \mathrm{Im}(\varphi)d) \mapsto (\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi))(u, d) \ .$$

It is immediate to check that ϑ is well defined. We prove now that ϑ is continuous. Let $V \subseteq (U \times D)/(\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi))$ be an open subset. Then $q^{-1}(V)$ is open $U \times D$. Let $(u, \mathrm{Im}(\varphi)d) \in \vartheta^{-1}(V)$. Then $q((u, d)) = \vartheta((u, \mathrm{Im}(\varphi)d)) \in V$ and so $(u, d) \in q^{-1}(V)$. Since $q^{-1}(V)$ is open, by definition of product topology there exists an open subset $U' \subseteq U$ such that $u \in U'$ and $U' \times \{d\} \subseteq q^{-1}(V)$ (recall that D has the discrete topology). Let $u' \in U'$. Then $\vartheta((u', \mathrm{Im}(\varphi)d)) = (\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi))(u', d) = q((u', d)) \in V$. So $(u', \mathrm{Im}(\varphi)d) \in \vartheta^{-1}(V)$. This shows that $U' \times \{\mathrm{Im}(\varphi)d\} \subseteq \vartheta^{-1}(V)$. We have that $(u, \mathrm{Im}(\varphi)d) \in U' \times \{\mathrm{Im}(\varphi)d\}$ and, by definition of product topology, $U' \times \{\mathrm{Im}(\varphi)d\}$ is open in $U \times (D/\mathrm{Im}(\varphi))$, because $D/\mathrm{Im}(\varphi)$ has the discrete topology. So $\vartheta^{-1}(V)$ is open. This proves that ϑ is continuous. It is obvious that ϑ is bijective, with inverse

$$\vartheta^{-1} : (U \times D)/(\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi)) \to U \times (D/\mathrm{Im}(\varphi)), \\ (\{\mathrm{id}_U\} \times \mathrm{Im}(\varphi))(u, d) \mapsto (u, \mathrm{Im}(\varphi)d) \ ,$$

which is immediately checked to be well defined. Moreover, ϑ^{-1} is continuous, because its components are continuous. Then ϑ is a homeomorphism. Now we have a homeomorphism $\vartheta^{-1} \circ \overline{\alpha} : \left(\overline{f}\right)^{-1}(U) \to U \times (D/\operatorname{Im}(\varphi))$ and $D/\operatorname{Im}(\varphi)$ is a finite discrete topological space. Denote by $q_U : U \times (D/\operatorname{Im}(\varphi)) \to U$ the projection on the first factor. By definition of ϑ, we have that $q_U \circ \vartheta^{-1} \circ q = p_U$. Then we have

$$(q_U \circ \vartheta^{-1} \circ \overline{\alpha}) \circ p = q_U \circ \vartheta^{-1} \circ q \circ \alpha = p_U \circ \alpha = f = \overline{f} \circ p ,$$

which implies that $q_U \circ (\vartheta^{-1} \circ \overline{\alpha}) = \overline{f}$ (by uniqueness in the universal property of the quotient of sets). So $\overline{f}$ is a finite covering of X. Since $f = \overline{f} \circ p$, we have that p is a morphism of coverings from f to $\overline{f}$. We have also that $\overline{f} \circ \sigma = \overline{f}$, for any $\sigma \in G$. Let now Z be a topological space and $g : Z \to X$ a finite covering, with a morphism of coverings $l : Y \to Z$ such that $l \circ \sigma = l$ for any σ in G. As in example 1.1.3(5), we have a unique map $\overline{l} : Y/G \to Z$ such that $l = \overline{l} \circ p$. This map is continuous by definition of quotient topology, because $l = \overline{l} \circ p$ is continuous. Moreover, since l is a morphism of coverings, we have that $g \circ l = f$ and so $g \circ \overline{l} \circ p = g \circ l = f = \overline{f} \circ p$. This implies that $g \circ \overline{l} = \overline{f}$. So $\overline{l}$ is a morphism of coverings from $\overline{f}$ to g. Hence $\overline{f} : Y/G \to X$ is the quotient of f by G in $\mathbf{Cov}_X$.

(G3) Let $f : Y \to X$, $g : Z \to X$ be finite coverings and $h : Y \to Z$ a morphism of coverings. Consider $\operatorname{Im}(h) \subseteq Z$ with the subspace topology and define $g' = g : \operatorname{Im}(h) \to X$. Then g' is continuous, because it is the restriction of a continuous function. Moreover, $g' = g \circ u'$, where $u' : \operatorname{Im}(h) \to Z$ is the canonical inclusion (continuous by definition of the subspace topology). We claim that g' is a finite covering of X. Let $x' \in X$. By lemma 1.5, there exists an open neighbourhood U of x' in X such that f, g and h are trivial above U. This means that we have finite discrete topological spaces D and E, homeomorphisms $\alpha : f^{-1}(U) \to U \times D$ and $\beta : g^{-1}(U) \to U \times E$ and a map $\varphi : D \to E$ such that $\beta \circ h = (\mathrm{id}_U \times \varphi) \circ \alpha$, $f = p_U \circ \alpha$ and $g = q_U \circ \beta$, where $p_U : U \times D \to U$ and $q_U : U \times E \to U$ are the projections to the first factor. We have that $(g')^{-1}(U) = \{z \in \operatorname{Im}(h) \mid g(z) = g'(z) \in U\} = \operatorname{Im}(h) \cap g^{-1}(U)$. Let $z \in (g')^{-1}(U) = \operatorname{Im}(h) \cap g^{-1}(U)$. Then $g(z) \in U$ and there exists $y \in Y$ such that $z = h(y)$. Since h is a morphism of coverings, we have that $f = g \circ h$. So $f(y) = g(h(y)) = g(z) \in U$, i.e. $y \in f^{-1}(U)$. Since $f = p_U \circ \alpha$, we have that $\alpha(y) = (f(y), d)$, for a $d \in D$. Then, since $\beta \circ h = (\mathrm{id}_U \times \varphi) \circ \alpha$, we have that

$$\begin{aligned}\beta(z) = \beta(h(y)) = (\mathrm{id}_U \times \varphi)(\alpha(y)) = \\ = (\mathrm{id}_U \times \varphi)((f(y), d)) = (f(y), \varphi(d)) \in U \times \operatorname{Im}(\varphi) .\end{aligned}$$

This shows that $\beta((g')^{-1}(U)) \subseteq U \times \operatorname{Im}(\varphi)$. Conversely, let $(u, e) \in U \times \operatorname{Im}(\varphi)$. Then $e \in \operatorname{Im}(\varphi)$, i.e. there exists $d \in D$ such that $e = \varphi(d)$. So, if we set $y := \alpha^{-1}((u, d))$, we have

$$(u, e) = (\mathrm{id}_U \times \varphi)((u, d)) = (\mathrm{id}_U \times \varphi)(\alpha(y)) = \beta(h(y)) \in \beta(\operatorname{Im}(h)) .$$

So $\beta((g')^{-1}(U)) = U \times \mathrm{Im}(\varphi)$. Then, restricting β to $(g')^{-1}(U)$, we get a homeomorphism $\beta : (g')^{-1}(U) \to U \times \mathrm{Im}(\varphi)$. Notice that $\mathrm{Im}(\varphi) \subseteq E$ is a finite discrete topological space. Moreover, since $g = q_U \circ \beta$, we have also $g' = q'_U \circ \beta$, where $q'_U : U \times \mathrm{Im}(\varphi) \to U$ is the projection on the first factor. So g' is a finite covering of X. Since $g' = g \circ u'$, we have that u' is a morphism of coverings from g' to g. Define also $u'' = h : Y \to \mathrm{Im}(h)$, which is continuous since h is continuous. We have $g' \circ u'' = g \circ h = f$, so u'' is a morphism of coverings from f to g'. Clearly we have that $f = u' \circ u''$. Moreover, u'' is surjective, so it is an epimorphism in $\mathbf{Cov}_X$, by lemma 1.7. It remains to prove that u' is a monomorphism in $\mathbf{Cov}_X$. We have that u' is injective, so it is a monomorphism of sets, by example 1.1.3(6) (notice that in the proof we did not use the fact that the sets were finite, so it works for arbitrary sets). Let W be a topological space and $m : W \to X$ a finite covering. Let $l_1, l_2 : W \to \mathrm{Im}(h)$ be two morphisms of coverings such that $u' \circ l_1 = u' \circ l_2$. In particular, l_1, l_2 are maps between sets. Since h is a monomorphism of sets, this implies that $l_1 = l_2$.
Assume now that h is a monomorphism in $\mathbf{Cov}_X$. We claim that h is injective. By the proof of (G1), we have that $m = f \circ p_1 = f \circ p_2 : Y \times_Z Y \to X$ is a finite covering of X, where $p_1 : Y \times_Z Y \to Y$, $p_2 : Y \times_Z Y \to Y$ are the two projections, which are morphisms of coverings from m to f. By definition of fibred product, we have that $h \circ p_1 = h \circ p_2$. Since h is a monomorphism in $\mathbf{Cov}_X$, this implies that $p_1 = p_2$. Let now $y_1, y_2 \in Y$ such that $h(y_1) = h(y_2)$. Then $(y_1, y_2) \in Y \times_Z Y$. So we have $y_1 = p_1((y_1, y_2)) = p_2((y_1, y_2)) = y_2$. This proves that h is injective. Then $h : Y \to \mathrm{Im}(h)$ is bijective. We claim that it is a homeomorphism. We already know that h is continuous, so it is enough to prove that it is open. Let $V \subseteq Y$ be open and let $z \in h(V)$. Then there exists $y \in V$ such that $z = h(y)$. Define $x' := g(z) \in X$ and consider U, D, E, α, β and φ as above. Then $z \in g^{-1}(U)$. Since $f = g \circ h$, we have that $f(y) = g(h(y)) = g(z) = x'$, which implies that $y \in f^{-1}(U) \cap V$. Since V is open in Y, we have that $V \cap f^{-1}(U)$ is open in $f^{-1}(U)$. Then $\alpha(V \cap f^{-1}(U))$ is open in $U \times D$, because α is a homeomorphism. Since $f = p_U \circ \alpha$, we have that $\alpha(y) = (f(y), d) = (x', d)$, for a $d \in D$. Then $(x', d) \in \alpha(V \cap f^{-1}(U))$. By definition of product topology, there exists an open neighbourhood U' of x' in X such that $U' \times \{d\} \subseteq \alpha(V \cap f^{-1}(U))$ (recall that D has the discrete topology). Define $e := \varphi(d) \in E$. Since $\beta \circ h = (\mathrm{id}_U \times \varphi) \circ \alpha$, we have that

$$\beta(z) = \beta(h(y)) = (\mathrm{id}_U \times \varphi)(\alpha(y)) = (\mathrm{id}_U \times \varphi)((x', d)) = (x', e) .$$

So $\beta(z) \in U' \times \{e\}$ and $z \in \beta^{-1}(U' \times \{e\})$. Let $x'' \in U'$. Then $(x'', d) \in U' \times \{d\} \subseteq \alpha(V \cap f^{-1}(U))$, which implies that $\alpha^{-1}((x'', d)) \in V \cap f^{-1}(U)$. So

$$(x'', e) = (\mathrm{id}_U \times \varphi)((x', d)) = \beta(h(\alpha^{-1}((x'', d)))) \in \beta(h(V)) .$$

This shows that $U' \times \{e\} \subseteq \beta(h(V))$, so $\beta^{-1}(U' \times \{e\}) \subseteq h(V)$. We have that $U' \times \{e\}$ is open in $U \times E$, because E has the discrete topology. Then $\beta^{-1}(U' \times \{e\})$ is open in Z. This proves that V is open. So $h : Y \to \mathrm{Im}(h)$ is a homeomorphism. Consider the finite covering $g' : \mathrm{Im}(h) \to X$ as above. We have that $f = g \circ h = g' \circ h$, so h is a morphism of coverings from f to g'. Since

$h : Y \to \mathrm{Im}(h)$ is a homeomorphism, we have that h^{-1} is also continuous. We have $f \circ h^{-1} = g'$ and so h^{-1} is a morphism of coverings from g' to f. This proves that $f : Y \to X$ and $g' : \mathrm{Im}(h) \to X$ are isomorphic in $\mathbf{Cov}_X$. It remains to prove that g' (together with the canonical inclusion) is a direct summand of $g : Z \to X$. Consider $W := Z \backslash \mathrm{Im}(h)$ and $g'' = g : W \to X$. Clearly, g'' is continuous, because it is the restriction of a continuous function. We claim that $g'' : W \to X$ is a finite covering. Let $x' \in X$ and consider U, D, E, α, β and φ as above. Then

$$(g'')^{-1}(U) = \{z \in W \mid g(z) = g''(z) \in U\} = W \cap g^{-1}(U) =$$
$$= (Z \backslash \mathrm{Im}(h)) \cap g^{-1}(U) = g^{-1}(U) \backslash (\mathrm{Im}(h) \cap g^{-1}(U)) = g^{-1}(U) \backslash \left((g')^{-1}(U)\right)$$

(see above for the last equality). As above, we have $\beta((g')^{-1}(U)) = U \times \mathrm{Im}(\varphi)$. Then, since β is a homeomorphism, we have that

$$\beta((g'')^{-1}(U)) = \beta\left(g^{-1}(U) \backslash \left((g')^{-1}(U)\right)\right) =$$
$$= \beta(g^{-1}(U)) \backslash \beta((g')^{-1}(U)) = (U \times E) \backslash (U \times \mathrm{Im}(\varphi)) = U \times (E \backslash \mathrm{Im}(\varphi)) \ .$$

Then, restricting β to $(g'')^{-1}(U)$, we get a homeomorphism

$$\beta : (g'')^{-1}(U) \to U \times (E \backslash \mathrm{Im}(\varphi)) \ .$$

Notice that $E \backslash \mathrm{Im}(\varphi) \subseteq E$ is a discrete topological set. Moreover, since $g = q_U \circ \beta$, we have also $g'' = q''_U \circ \beta$, where $q''_U : U \times (E \backslash \mathrm{Im}(\varphi)) \to U$ is the projection on the first factor. So g'' is a finite covering of X. We have that $Z = \mathrm{Im}(\varphi) \amalg (Z \backslash \mathrm{Im}(\varphi)) = \mathrm{Im}(\varphi) \amalg W$ as sets. By lemma 1.7, we have that $\mathrm{Im}(\varphi)$ is both open and closed in Z. So the topology of Z coincides with the disjoint union topology. Then we have that g, together with the canonical inclusions $\mathrm{Im}(\varphi) \to Z$ and $W \to Z$, is the sum of g' and g'', as in the proof of (G2).

(G4) We have that $F_x(\mathrm{id}_X) = \mathrm{id}_X^{-1}(\{x\}) = \{x\}$, which is terminal in **sets** (example 1.1.3(1)). So F_x transforms the terminal object id_X (see the proof of (G1)) in the terminal object $\{x\}$.
Let $f_1 : Y_1 \to X$, $f_2 : Y_2 \to X$, $g : Z \to X$ be finite coverings, $h_1 : Y_1 \to Z$ and $h_2 : Y_2 \to Z$ two morphisms of coverings. In the proof of (G1), we saw that $f : Y_1 \times_Z Y_2 \to X$ is the fibred product of f_1 and f_2 over Z in $\mathbf{Cov}_X$. For any $(y_1, y_2) \in Y_1 \times_Z Y_2$, we have that $f((y_1, y_2)) = f_1(y_1) = f_2(y_2)$. Then

$$f^{-1}(\{x\}) = \{(y_1, y_2) \in Y_1 \times_Z Y_2 \mid f((y_1, y_2)) = x\} =$$
$$= \{(y_1, y_2) \in Y_1 \times Y_2 \mid h_1(y_1) = h_2(y_2),\ f_1(y_1) = x,\ f_2(y_2) = x\} =$$
$$= \{(y_1, y_2) \in f_1^{-1}(\{x\}) \times f_2^{-1}(\{x\}) \mid h_1(y_1) = h_2(y_2)\} =$$
$$= f_1^{-1}(\{x\}) \times_Z f_2^{-1}(\{x\}) = f_1^{-1}(\{x\}) \times_{g^{-1}(\{x\})} f_2^{-1}(\{x\})$$

(in the last equality we used the fact that $h_1(f_1^{-1}(\{x\})) \subseteq g^{-1}(\{x\})$ and $h_2(f_2^{-1}(\{x\})) \subseteq g^{-1}(\{x\})$). So

$$F_x(f_1 \times_g f_2) = F_x(f) = f^{-1}(\{x\}) =$$
$$= f_1^{-1}(\{x\}) \times_{g^{-1}(\{x\})} f_2^{-1}(\{x\}) = F_x(f_1) \times_{F_x(g)} F_x(f_2) \ ,$$

which is what we needed.

(G5) Let $(f_i : Y_i \to X)_{i\in I}$ be a finite collection of finite coverings of X and define $Y := \coprod_{i\in I} Y_i$. In the proof of (G2), we saw that $f : Y \to X,\ y \mapsto f_j(y)$, where j is the unique element of I such that $y \in Y_j$, is the sum of the f_i's in $\mathbf{Cov}_X$. We have that

$$f^{-1}(\{x\}) = \left\{ y \in Y = \coprod_{i\in I} Y_i \;\middle|\; f(y) = x \right\} = \\ = \coprod_{i\in I} \{y \in Y_i \mid f_j(y) = f(y) = x\} = \coprod_{i\in I} f_i^{-1}(\{x\}) \ .$$

So $F_x(f) = f^{-1}(\{x\}) = \coprod_{i\in I} f_i^{-1}(\{x\}) = \coprod_{i\in I} F_x(f_i)$, which is what we needed, since the disjoint union is the sum in **sets** (see example 1.1.3(3)).
Let now $f : Y \to X$ be a finite covering and G a finite subgroup of $\mathrm{Aut}_{\mathbf{Cov}_X}(f)$. In the proof of (G2), we saw that $\overline{f} : Y/G \to X,\ Gy \mapsto f(y)$ is the quotient of f by G in $\mathbf{Cov}_X$. Notice that $F_x(G) = \left\{ \sigma_{|_{F_x(\overline{f})}} \;\middle|\; \sigma \in G \right\}$. We have that

$$\left(\overline{f}\right)^{-1}(\{x\}) = \{Gy \in Y/G \mid f(y) = \overline{f}(Gy) = x\} = \\ = \{Gy \in Y/G \mid y \in f^{-1}(\{x\})\} = f^{-1}(\{x\})/F_x(G) \ .$$

So $F_x\left(\overline{f}\right) = \left(\overline{f}\right)^{-1}(\{x\}) = f^{-1}(\{x\})/F_x(G) = F_x(f)/F_x(G)$, which is what we needed (see example 1.1.3(5)).
Let $f : Y \to X$, $g : Z \to X$ be finite coverings and $h : Y \to Z$ an epimorphism of coverings. By lemma 1.7, h is surjective. Let $z \in F_x(g) = g^{-1}(\{x\}) \subseteq Z$. Then $g(z) = x$. Moreover, since h is surjective, there exists $y \in Y$ such that $z = h(y)$. Since h is a morphism of coverings, we have that $f = g \circ h$. Then $f(y) = g(h(y)) = g(z) = x$. So $y \in f^{-1}(\{x\}) = F_x(f)$. We have that $F_x(h)(y) = h(y) = z$. This shows that $F_x(h) : F_x(f) \to F_x(g)$ is surjective, i.e. an epimorphism in **sets** (see example 1.1.3(6)).

(G6) Let $f : Y \to X$, $g : Z \to X$ be finite coverings of X and $h : Y \to Z$ a morphism of coverings such that $F_x(h)$ is an isomorphism of sets, i.e. a bijection. Define $A := \{x' \in X \mid F_{x'}(h) \text{ is bijective}\} \subseteq X$. We claim that A is both open and closed in X. Let $x' \in A$, i.e. $F_{x'}(h)$ is bijective. By lemma 1.5, there exists an open neighbourhood U of x' in X such that f, g and h are trivial above U. This means that there exist finite discrete topological spaces D and E, homeomorphisms $\alpha : f^{-1}(U) \to U \times D$ and $\beta : g^{-1}(U) \to U \times E$ and a map $\varphi : D \to E$ such that $\beta \circ h = (\mathrm{id}_U \times \varphi) \circ \alpha$, $f = p_U \circ \alpha$ and $g = q_U \circ \beta$, where $p_U : U \times D \to U$ and $q_U : U \times E \to U$ are the projections to the first factor. Since $f = p_U \circ \alpha$, we have that

$$\alpha(f^{-1}(\{x'\})) = \alpha((p_U \circ \alpha)^{-1}(\{x'\})) = \\ = \alpha(\alpha^{-1}(p_U^{-1}(\{x'\}))) = p_U^{-1}(\{x'\}) = \{x'\} \times D$$

(we applied the fact that α is a homeomorphism). Analogously, it can be proved that $\beta(g^{-1}(\{x'\})) = \{x'\}\times E$. Since $F_{x'}(h) = h : F_{x'}(f) = f^{-1}(\{x'\}) \to F_{x'}(g) = g^{-1}(\{x'\})$ is bijective and $\mathrm{id}_U \times\varphi = \beta\circ h\circ\alpha^{-1}$, we have that $\mathrm{id}_U \times\varphi : \alpha(f^{-1}(\{x'\})) = \{x'\} \times D \to \beta(g^{-1}(\{x'\})) = \{x'\} \times E$ is bijective. This means that φ is bijective. Then $\beta\circ h\circ\alpha^{-1} = \mathrm{id}_U \times\varphi : U\times D \to U\times E$ is bijective, which implies that $h : f^{-1}(U) \to g^{-1}(U)$ is bijective (since β and α are both bijective). Let now $x'' \in U$. We know that $h(f^{-1}(\{x''\})) \subseteq g^{-1}(\{x''\})$. Conversely, let $z \in g^{-1}(\{x''\}) \subseteq g^{-1}(U)$, i.e. $g(z) = x''$. Since $h : f^{-1}(U) \to g^{-1}(U)$ is bijective, there exists $y \in f^{-1}(U)$ such that $z = h(y)$. Since $f = g \circ h$, we have that $f(y) = g(h(y)) = g(z) = x''$. So $y \in f^{-1}(\{x''\})$ and $z = h(y) \in h(f^{-1}(\{x''\}))$. Then $h(f^{-1}(\{x''\})) = g^{-1}(\{x''\})$. So, restricting the bijection $h : f^{-1}(U) \to g^{-1}(U)$ to $f^{-1}(\{x''\})$, we get a bijection $h : F_{x''}(f) = f^{-1}(\{x''\}) \to F_{x''}(g) = g^{-1}(\{x''\})$, which by definition of $F_{x''}$ coincides with $F_{x''}(h)$. So $F_{x''}(h)$ is bijective, which means that $x'' \in A$. Then $U \subseteq A$. So A is open.
On the other hand, let $x' \in X\backslash A$. If by contradiction there exists $x'' \in U \cap A$, then the same argument as above shows that $U \subseteq A$. But $x \notin A$, so this is a contradiction. This means that $U \cap A = \emptyset$, i.e. $U \subseteq X\backslash A$. Then $X\backslash A$ is open, i.e. A is closed.
So A is both open and closed. But X is connected. Then we must have either $A = \emptyset$ or $A = X$. Since $x \in A$, we have that $A \neq \emptyset$ and so $A = X$. This means that $F_{x'}(h)$ is bijective for any $x' \in X$. Let $y_1, y_2 \in Y$ such that $h(y_1) = h(y_2)$. Then, since $f = g \circ h$, we have that $f(y_1) = g(h(y_1)) = g(h(y_2)) = f(y_2)$. Define $x' := f(y_1) = f(y_2) \in X$. Then $y_1, y_2 \in f^{-1}(\{x'\}) = F_{x'}(f)$ and $F_{x'}(h)(y_1) = h(y_1) = h(y_2) = F_{x'}(h)(y_2)$. Since $F_{x'}(h)$ is bijective, we must have $y_1 = y_2$. So h is injective. Let $z \in Z$ and define $x' := g(z)$. Then $z \in g^{-1}(\{x'\}) = F_{x'}(g)$. Since $F_{x'}(h) : F_{x'}(f) \to F_{x'}(g)$ is bijective, there exists $y \in F_{x'}(f) = f^{-1}(\{x'\}) \subseteq Y$ such that $z = F_{x'}(h)(y) = h(y)$. So h is surjective. Now we know that h is bijective and continuous. As in the proof of (G3), it can be proved that h is open. So $h : Y \to Z$ is a homeomorphism. Since $f = g \circ h$, we have that $f \circ h^{-1} = g$. This shows that also $h^{-1} : Z \to Y$ is a morphism of coverings. Hence h is an isomorphism in $\mathbf{Cov}_X$.

□

Remark 1.9. In the proof of proposition 1.8, the point where we applied the fact that X is connected was (G6). In fact, the axiom (G6) is never satisfied if $X \neq \emptyset$ is not connected. In that case we can write X as the topological disjoint union $X_1 \amalg X_2$, with $X_1 \neq \emptyset$ and $X_2 \neq \emptyset$. Then we can consider the finite covering $f : Y := (X_1 \times \{1\}) \amalg (X_2 \times \{1, 2\}) \to X$. The map $h : X \to Y$, $x \mapsto (x, 1)$ is a morphism of coverings from $\mathrm{id}_X : X \to X$ to $f : Y \to X$. It is clear that h is not bijective, so it cannot be an isomorphism of coverings. However, if we take $x \in X_1$, we have that $F_x(h) : F_x(\mathrm{id}_X) = \{x\} \to F_x(f) = \{(x, 1)\}$ is bijective. Hence $\mathbf{Cov}_X$ is Galois with fundamental functor F_x (for any $x \in X$) if and only if X is connected.

Corollary 1.10. *Let X be a connected topological space. Then there exists a profinite group $\hat{\pi}(X)$, uniquely determined up to isomorphism, such that $\mathbf{Cov}_X$ is equivalent* *to* $\hat{\pi}(X)$-**sets**. *Moreover,* $\hat{\pi}(X)$ *is isomorphic to* $\mathrm{Aut}(F_x)$ *for any* $x \in X$*, where* $F_x : \mathbf{Cov}_X \to \mathbf{sets}$ *is defined as in lemma 1.3.*

Proof. It follows immediately from the proposition 1.8 and from the main theorem about Galois categories (1.4.34). □

Definition 1.11. If X is a connected topological space, for any $x \in X$ we define $\hat{\pi}(X, x) := \mathrm{Aut}(F_x)$ the *fundamental group of X in x*, where $F_x : \mathbf{Cov}_X \to \mathbf{sets}$ is the functor defined in 1.3.

Remark 1.12. (1) In topology we have another definition of fundamental group: for any topological space $X \neq \emptyset$ and any $x \in X$ we denote by $\pi(X, x)$ the group of homotopy classes of loops with base point x. If X is path-connected, this group does not depend on the base point and is denoted by $\pi(X)$. If X satisfies stronger connectdness assumptions (connected, locally path-connected and semilocally simply connected), then a theorem in algebraic topology states that the category of coverings of X (all coverings, not only the finite ones) is equivalent to the category of $\pi(X)$-sets (also here, all $\pi(X)$-sets, not only the finite ones). The similarity between this result and corollary 1.10 suggests that there might be a link between $\pi(X)$ and $\hat{\pi}(X)$ (but notice that $\pi(X)$ is just a group, not a profinite group). Indeed, such a link exists: it can be proved that $\hat{\pi}(X)$ is the profinite completion of $\pi(X)$ (see 2.4 for the definition of profinite completion).

(2) The fundamental group defined as in 1.11 is functorial in (X, x). More precisely, we can consider the category $\mathbf{Conn}_\bullet$ of pointed connected topological spaces, whose objects are pairs of the form (X, x), with X connected and $x \in X$ (*base point*), and morphisms are continuous functions that send the base point of a space into the base point of the other space. To any object (X, x) of $\mathbf{Conn}_\bullet$ we can associate the Galois category $\mathbf{Cov}_X$ with fundamental functor $F_x : \mathbf{Cov}_X \to \mathbf{sets}$. If we show that the assumptions of lemma 1.4.36 are satisfied, then we can extend $\hat{\pi}$ to a functor $\mathbf{Conn}_\bullet \to \mathbf{Prof}$.
Let (X, x), (Y, y) be two objects of $\mathbf{Conn}_\bullet$ and $f : (X, x) \to (Y, y)$ a morphism in $\mathbf{Conn}_\bullet$, i.e. f is continuous and $f(x) = y$. Then we can define a functor $G_f : \mathbf{Cov}_Y \to \mathbf{Cov}_X$ as follows. If $g : Z \to Y$ is a finite covering of Y, we can consider the fibred product $X \times_Y Z$ with the projection $p_1 : X \times_Y Z \to X$. Let us prove that p_1 is a finite covering of X. Let $x' \in X$. Since $f(x') \in Y$ and $g : Z \to Y$ is a finite covering of Y, there exist an open neighbourhood U of $f(x')$ in Y, a discrete topological space E and a homeomorphism $\varphi : g^{-1}(U) \to U \times E$ such that $p_U \circ \varphi = g$, where $p_U : U \times E \to U$ is the projection on the first factor. Since f is continuous, $f^{-1}(U)$ is an open subset of X. Moreover, since $f(x') \in U$, we have that $x' \in f^{-1}(U)$. So $f^{-1}(U)$ is an open neighbourhood of x' in X. We have that

$$p_1^{-1}(f^{-1}(U)) = \{(x'', z) \in X \times_Y Z \mid x'' = p_1((x'', z)) \in f^{-1}(U)\} =$$
$$= \{(x'', z) \in X \times Z \mid g(z) = f(x'') \in U\} =$$
$$= \{(x'', z) \in f^{-1}(U) \times g^{-1}(U) \mid g(z) = f(x'')\} = f^{-1}(U) \times_U g^{-1}(U) \,.$$

Define

$$\psi : p_1^{-1}(f^{-1}(U)) = f^{-1}(U) \times_U g^{-1}(U) \to f^{-1}(U) \times E,$$
$$(x'', z) \mapsto (x'', p_E(\varphi(z))) \,,$$

where $p_E : U \times E \to E$ is the projection on the second factor (which is continuous by definition of product topology). We have that ψ is continuous, because its components are continuous. Moreover, define

$$\psi' : f^{-1}(U) \times E \to p_1^{-1}(f^{-1}(U)) = f^{-1}(U) \times_U g^{-1}(U),$$
$$(x'', e) \mapsto (x'', \varphi^{-1}((f(x''), e))) \,.$$

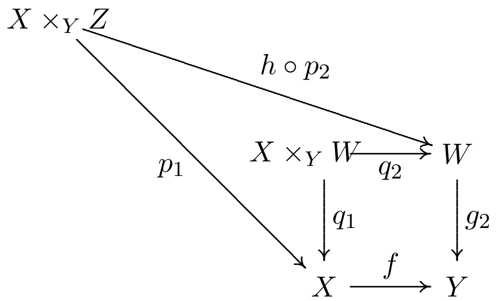
This is well defined, because for any $x'' \in f^{-1}(U)$, $e \in E$ we have that $g(\varphi^{-1}((f(x''), e))) = p_U((f(x''), e)) = f(x'')$ (we used the fact that $p_U \circ \varphi = g$) and so $(x'', \varphi^{-1}((f(x''), e))) \in f^{-1}(U) \times_U g^{-1}(U)$. We have that ψ' is also continuous, because its components are continuous. Moreover, we have that

$$\begin{aligned}\psi'(\psi((x'', z))) &= \psi'((x'', p_E(\varphi(z)))) = \\ &= (x'', \varphi^{-1}((f(x''), p_E(\varphi(z))))) = (x'', \varphi^{-1}((g(z), p_E(\varphi(z))))) = \\ &= (x'', \varphi^{-1}((p_U(\varphi(z)), p_E(\varphi(z))))) = (x'', \varphi^{-1}(\varphi(z))) = (x'', z)\end{aligned}$$

for any $(x'', z) \in f^{-1}(U) \times_U g^{-1}(U)$. So $\psi' \circ \psi = \mathrm{id}_{f^{-1}(U) \times_U g^{-1}(U)}$. Conversely,

$$\begin{aligned}\psi(\psi'((x'', e))) &= \psi((x'', \varphi^{-1}((f(x''), e)))) = \\ &= (x'', p_E(\varphi(\varphi^{-1}((f(x''), e))))) = (x'', p_E((f(x''), e))) = (x'', e)\end{aligned}$$

for any $x'' \in f^{-1}(U)$, $e \in E$. So $\psi \circ \psi' = \mathrm{id}_{f^{-1}(U) \times E}$. This shows that ψ and ψ' are inverse to each other. So ψ is a homeomorphism. Moreover, by definition we have that $p_{f^{-1}(U)} \circ \psi = p_1$, where $p_{f^{-1}(U)} : f^{-1}(U) \times E \to f^{-1}(U)$ is the projection on the first factor. Then $p_1 : X \times_Y Z \to X$ is a finite covering of X and we can define $G_f(g : Z \to Y) = (p_1 : X \times_Y Z \to X)$.
If $g_1 : Z \to Y$, $g_2 : W \to Y$ are two finite coverings and $h : Z \to W$ is a morphism of coverings, then consider the following diagram, where $p_1 : X \times_Y Z \to X$, $p_2 : X \times_Y Z \to Z$, $q_1 : X \times_Y W \to X$ and $q_2 : X \times_Y W \to W$ are the projections.



Since h is a morphism of coverings, we have that $g_1 = g_2 \circ h$ and so (using the definition of fibred product) $f \circ p_1 = g_1 \circ p_2 = g_2 \circ h \circ p_2$. Then the diagram is commutative and, by the universal property of the fibred product, there exists

a unique continuous map $h' : X \times_Y Z \to X \times_Y W$ such that $q_1 \circ h' = p_1$ and $q_2 \circ h' = h \circ p_2$. The fact that $q_1 \circ h' = p_1$ means that h' is a morphism of coverings from $p_1 = G_f(g_1 : Z \to Y)$ to $q_1 = G_f(g_2 : W \to Y)$. So we can define $G_f(h) = h'$. It is easy to prove that G_f is a functor, using uniqueness in the universal property of the fibered product.
Let $F_x : \mathbf{Cov}_X \to \mathbf{sets}$ and $F_y : \mathbf{Cov}_Y \to \mathbf{sets}$ be defined as in lemma 1.3. If $g : Z \to Y$ is a finite covering of Y, we have that

$$F_x(G_f(g)) = G_f(g)^{-1}(\{x\}) = \{(x', z) \in X \times_Y Z \mid x' = G_f(g)((x', z)) = x\} =$$
$$= \{(x, z) \mid z \in Z,\ g(z) = f(x) = y\} = \{x\} \times g^{-1}(\{y\}) = \{x\} \times F_y(g)$$

(we used the fact that $f(x) = y$). So we have a bijection

$$\alpha_{f,g} : F_x(G_f(g)) = \{x\} \times F_y(g) \to F_y(g),\ (x, z) \mapsto z\ .$$

If $g_1 : Z \to Y$, $g_2 : W \to Y$ are two finite coverings and $h : Z \to W$ is a morphism of coverings, consider the following diagram.

$$\begin{array}{ccc} F_x(G_f(g_1)) = \{x\} \times F_y(g_1) & \xrightarrow{\alpha_{f,g_1}} & F_y(g_1) \\ {\scriptstyle F_x(G_f(h))}\downarrow & & \downarrow{\scriptstyle F_y(h)} \\ F_x(G_f(g_2)) = \{x\} \times F_y(g_2) & \xrightarrow{\alpha_{f,g_2}} & F_y(g_2) \end{array}$$

For any $z \in F_y(g_1)$, we have that

$$F_y(h)(\alpha_{f,g_1}((x, z))) = F_y(h)(z) = h(z) = \alpha_{f,g_2}((x, h(z))) =$$
$$= \alpha_{f,g_2}(G_f(h)((x, z))) = \alpha_{f,g_2}(F_x(G_f(h))((x, z)))\ .$$

So $F_y(h) \circ \alpha_{f,g_1} = \alpha_{f,g_2} \circ G_f(F_x(h))$. Then $\alpha_f = (\alpha_{f,g})_{g \in \mathrm{Ob}(\mathbf{Cov}_Y)}$ is an isomorphism of functors from $F_x \circ G_f$ to F_y.
Let now (X, x) be an object of $\mathbf{Conn}_\bullet$. Let $g : Y \to X$ be a finite covering of X and let $p_1 : X \times_X Y \to X$, $p_2 : X \times_X Y \to Y$ be the two projections. Then $G_{\mathrm{id}_X}(g) = p_1$, by definition. We have that

$$X \times_X Y = \{(x', y) \in X \times Y \mid x' = \mathrm{id}_X(x') = g(y)\}\ .$$

Then p_2 is a bijection, with inverse

$$p_2^{-1} : Y \to X \times_X Y,\ y \mapsto (g(y), y)\ .$$

We have that p_2 is continuous by definition of the topology on the fibred product and p_2^{-1} is continuous because its components are continuous. Moreover, by definition of fibred product we have that $g \circ p_2 = \mathrm{id}_X \circ p_1 = p_1$ and so also $g = p_1 \circ p_2^{-1}$. This means that p_2 is a morphism of coverings from p_1 to g and p_2^{-1} is a morphism of coverings from g to p_1. Then p_2 is an isomorphism of coverings from $p_1 = G_{\mathrm{id}_X}(g)$ to $g = \mathrm{id}_{\mathbf{Cov}_X}(g)$. Define $\beta_{(X,x),g} := p_2$. We claim that $\beta_{(X,x)} = (\beta_{(X,x),g})_{g \in \mathrm{Ob}(\mathbf{Cov}_X)}$ is an isomorphism of functors from G_{id_X} to $\mathrm{id}_{\mathbf{Cov}_X}$. We only have to check the compatibility condition. Let

$g_1 : Y \to X$, $g_2 : Z \to X$ be two finite coverings of X, with a morphism of coverings $h : Y \to Z$. Consider the following diagram, where $p_2 : X \times_X Y \to Y$ and $q_2 : X \times_X Z \to Z$ are the projections on the second factors.

$$\begin{array}{ccc} X \times_X Y & \xrightarrow{p_2} & Y \\ {\scriptstyle G_{\mathrm{id}_X}(h)}\downarrow & & \downarrow{\scriptstyle h} \\ X \times_X Z & \xrightarrow{q_2} & Z \end{array}$$

For any $(x', y) \in X \times_X Y$, we have that

$$q_2(G_{\mathrm{id}_X}(h)((x', y))) = q_2((x', h(y))) = h(y) = h(p_2((x', y))) \; .$$

So $\beta_{(X,x),g_1} \circ G_{\mathrm{id}_X}(h) = q_2 \circ G_{\mathrm{id}_X}(h) = h \circ p_2 = \mathrm{id}_{\mathbf{Cov}_X}(h) \circ \beta_{(X,x),g_2}$. This shows that $\beta_{(X,x)}$ is an isomorphism of functors from G_{id_X} to $\mathrm{id}_{\mathbf{Cov}_X}$. Moreover, let $g : Y \to X$ be a finite covering of X and consider $F_x(\beta_{(X,x),g}) : F_x(G_{\mathrm{id}_X}(g)) = \{x\} \times F_x(g) \to F_x(g)$. Using the definitions, for any $y \in F_x(g)$ we get that

$$F_x(\beta_{(X,x),g})((x, y)) = \beta_{(X,x),g}((x, y)) = y = \alpha_{\mathrm{id}_X,g}((x, y)) \; .$$

So $F_x(\beta_{(X,x),g}) = \alpha_{\mathrm{id}_X,g}$.
Let (X, x), (Y, y), (Z, z) be objects of $\mathbf{Conn}_\bullet$ with morphisms $f_1 : (X, x) \to (Y, y)$ and $f_2 : (Y, y) \to (Z, z)$. Let $g : W \to Z$ be a finite covering of Z. We have that

$$\begin{aligned} &X \times_Y (Y \times_Z W) = \{(x', (y', w)) \in X \times (Y \times_Z W) \mid f_1(x') = y'\} = \\ &= \{(x', (y', w)) \in X \times (Y \times W) \mid f_1(x') = y', (f_2 \circ f_1)(x') = f_2(y') = g(w)\} \end{aligned}$$

and

$$X \times_Z W = \{(x', w) \in X \times W \mid (f_2 \circ f_1)(x') = g(w)\} \; .$$

Then the map

$$\gamma_{f_1,f_2,g} : X \times_Y (Y \times_Z W) \to X \times_Z W, \; (x', (y', w)) \mapsto (x', w)$$

is a well-defined bijection, with inverse

$$\gamma^{-1}_{f_1,f_2,g} : X \times_Z W \to X \times_Y (Y \times_Z W), \; (x', w) \mapsto (x', (f_1(x'), w)) \; .$$

Both $\gamma_{f_1,f_2,g}$ and its inverse are continuous, because their components are continuous. Let $p_1 : X \times_Z W \to X$, $p_{11} : X \times_Y (Y \times_Z W) \to X$ and $p_{21} : Y \times_Z W \to Y$ be the projections on the first factors. Then $p_1 \circ \gamma_{f_1,f_2,g} = p_{11}$ and $p_{11} \circ \gamma^{-1}_{f_1,f_2,g} = p_1$. This means that $\gamma_{f_1,f_2,g}$ is a morphism of coverings from p_{11} to p_1 and $\gamma^{-1}_{f_1,f_2,g}$ is a morphism of coverings from p_1 to p_{11}. Then $\gamma_{f_1,f_2,g}$ is an isomorphism of coverings from $p_{11} = G_{f_1}(p_{21}) = G_{f_1}(G_{f_2}(g))$ to $p_1 = G_{f_2 \circ f_1}(g)$. We claim that $\gamma_{f_1,f_2} = (\gamma_{f_1,f_2,g})_{g \in \mathrm{Ob}(\mathbf{Cov}_Z)}$ is an isomorphism of functors from $G_{f_1} \circ G_{f_2}$ to $G_{f_2 \circ f_1}$. We only have to check the compatibility condition. Let $g_1 : W_1 \to Z$, $g_2 : W_2 \to Z$ be two finite coverings of Z, with a morphism of coverings $h : W_1 \to W_2$. Consider the following diagram.

$$\begin{array}{ccc}
X \times_Y (Y \times_Z W_1) & \xrightarrow{\gamma_{f_1,f_2,g_1}} & X \times_Z W_1 \\
{\scriptstyle (G_{f_1} \circ G_{f_2})(h)} \downarrow & & \downarrow {\scriptstyle G_{f_2 \circ f_1}(h)} \\
X \times_Y (Y \times_Z W_2) & \xrightarrow{\gamma_{f_1,f_2,g_2}} & X \times_Z W_2
\end{array}$$

For any $(x', (y', w)) \in X \times_Y (Y \times_Z W_1)$, we have that

$$\begin{aligned}
&\gamma_{f_1,f_2,g_2}(G_{f_1}(G_{f_2}(h))((x', (y', w)))) = \\
&\quad = \gamma_{f_1,f_2,g_2}((x', G_{f_2}(h)((y', w)))) = \gamma_{f_1,f_2,g_2}((x', (y', h(w)))) = \\
&\quad = (x', h(w)) = G_{f_2 \circ f_1}(h)((x', w)) = G_{f_2 \circ f_1}(h)(\gamma_{f_1,f_2,g}((x', (y', w)))) \,.
\end{aligned}$$

So $\gamma_{f_1,f_2,g_2} \circ (G_{f_1} \circ G_{f_2})(h) = G_{f_2 \circ f_1}(h) \circ \gamma_{f_1,f_2,g_1}$. This shows that γ_{f_1,f_2} is an isomorphism of functors from $G_{f_1} \circ G_{f_2}$ to $G_{f_2 \circ f_1}$. Finally, let $g : W \to Z$ be a finite covering of Z and consider the following diagram.

$$\begin{array}{ccc}
(F_x \circ G_{f_1} \circ G_{f_2})(g) & \xrightarrow{\alpha_{f_1, G_{f_2}(g)}} & (F_y \circ G_{f_2})(g) \\
{\scriptstyle F_x(\gamma_{f_1,f_2,g})} \downarrow & & \downarrow {\scriptstyle \alpha_{f_2,g}} \\
(F_x \circ G_{f_2 \circ f_1})(g) & \xrightarrow{\alpha_{f_2 \circ f_1, g}} & F_z(g)
\end{array}$$

If $p_{11} : X \times_Y (Y \times_Z W) \to X$ is defined as above, we have that

$$(F_x \circ G_{f_1} \circ G_{f_2})(g) = p_{11}^{-1}(\{x\}) = \{(x, (f_1(x), w)) \mid w \in W\} \,.$$

For any $w \in W$, we have

$$\begin{aligned}
&\alpha_{f_2 \circ f_1, g}(F_x(\gamma_{f_1,f_2,g})((x, (f_1(x), w)))) = \alpha_{f_2 \circ f_1, g}(\gamma_{f_1,f_2,g}((x, (f_1(x), w)))) = \\
&= \alpha_{f_2 \circ f_1, g}((x, w)) = w = \alpha_{f_2,g}((f_1(x), w)) = \alpha_{f_2,g}(\alpha_{f_1, G_{f_2}}((x, (f_1(x), w)))) \,.
\end{aligned}$$

Then $\alpha_{f_2 \circ f_1, g} \circ F_x(\gamma_{f_1,f_2,g}) = \alpha_{f_2,g} \circ \alpha_{f_1, G_{f_2}}$, i.e. the diagram is commutative. So the assumptions of lemma 1.4.36 are satisfied and we have a functor $\hat{\pi} : \mathbf{Conn}_\bullet \to \mathbf{Prof}$ such that $\hat{\pi}((X, x)) = \pi(\mathbf{Cov}_X, F_x) = \mathrm{Aut}(F_x) = \hat{\pi}(X, x)$ for any object (X, x) of $\mathbf{Conn}_\bullet$.

Example 1.13. Let X be a connected topological space and fix $x \in X$. Since $\mathbf{Cov}_X$ is an essentially small Galois category with fundamental functor F_x, we can apply to it all the results of the previous sections. For example, any object of $\mathbf{Cov}_X$ is the sum of its connected components (proposition 1.2.20). It is interesting to describe the connected objects of $\mathbf{Cov}_X$. We will prove that a finite covering $f : Y \to X$ is connected if and only if Y is connected. This explains why connected objects in Galois categories have this name.
First of all, assume that $f : Y \to X$ is a finite covering of X with Y connected. Let $g : Z \to X$ be another finite covering and $h : Z \to Y$ a monomorphism of coverings. We have to prove that either g is initial or h is an isomorphism. From the proof of (G2) in the proposition 1.8, it follows that the initial object in $\mathbf{Cov}_X$ is $\emptyset \to X$. Assume then that $Z \neq \emptyset$. By lemma 1.7(1), we have that $\mathrm{Im}(h)$ is both open and closed in Y. On the other hand, $\mathrm{Im}(h) \neq \emptyset$, because $Z \neq \emptyset$. Since Y is connected, this implies that $\mathrm{Im}(h) = Y$, i.e. h is surjective. By lemma 1.7(2), h is

an epimorphism in $\mathbf{Cov}_X$. By (G5) of the definition of Galois category, this implies that $F_x(h)$ is an epimorphism of sets, i.e. surjective. Since h is a monomorphism, we have that $F_x(h) : F_x(g) \to F_x(f)$ is injective, by corollary 1.2.10. So $F_x(h)$ is a bijection, i.e. an isomorphism of sets. By (G6) of the definition of Galois category, this implies that h is an isomorphism. Hence $f : Y \to X$ is connected.
Conversely, assume that $f : Y \to X$ is a connected object of $\mathbf{Cov}_X$. Let $A \subseteq Y$ be a subspace that is at the same time open and closed. Assume $A \neq \emptyset$. We want to prove that $A = Y$. Let $q : A \to Y$ be the canonical inclusion, which is continuous by definition of subspace topology. Then $f \circ q : A \to X$ is continuous. We claim that $f \circ q$ is a finite covering of X. Let $x' \in X$. Since f is a finite covering of X, there exist an open neighbourhood U of x' in X, a finite discrete topological space E and a homeomorphism $\varphi : f^{-1}(U) \to U \times E$ such that $f = p_U \circ \varphi$, where $p_U : U \times E \to U$ is the projection on the first factor. We have that $A \cap f^{-1}(U)$ is both open and closed in $f^{-1}(U)$, by definition of subspace topology. Then, since φ is a homeomorphism, $\varphi(A \cap f^{-1}(U))$ is both open and closed in $U \times E$. Define

$$E' := \{e \in E \mid (x', e) \in \varphi(A \cap f^{-1}(U))\} .$$

Let $e \in E'$. Since $\varphi(A \cap f^{-1}(U))$ is open, by definition of product topology there exists an open neighbourhood V_e of x' in X such that $V_e \times \{e\} \subseteq \varphi(A \cap f^{-1}(U))$. On the other hand, if $e \in E \backslash E'$ we have that $(x', e) \in (X \times E) \backslash \varphi(A \cap f^{-1}(U))$, which is open because $\varphi(A \cap f^{-1}(U))$ is closed. Then, by definition of product topology, there exists an open neighbourhood V_e of x' in X such that $V_e \times \{e\} \subseteq (X \times E) \backslash \varphi(A \cap f^{-1}(U))$. Now we have an open neighbourhood V_e of x' in X for any $e \in E$. Define $V := \bigcap_{e \in E}$. Since E is finite, V is an open neighbourhood of x' in X. Moreover, we have that

$$V \times E' = \bigcup_{e \in E'} (V \times \{e\}) \subseteq \bigcup_{e \in E'} (V_e \times \{e\}) \subseteq \varphi(A \cap f^{-1}(U))$$

and

$$V \times (E \backslash E') = \bigcup_{e \in E \backslash E'} (V \times \{e\}) \subseteq \bigcup_{e \in E \backslash E'} (V_e \times \{e\}) \subseteq (X \times E) \backslash \varphi(A \cap f^{-1}(U)) .$$

So $(V \times E) \cap \varphi(A \cap f^{-1}(U)) = V \times E'$. Consider now $(f \circ q^{-1})(V)$. We have that $(f \circ q)^{-1}(V) = q^{-1}(f^{-1}(V)) = A \cap f^{-1}(V)$, by definition of q. Then, since $f^{-1}(V) \subseteq f^{-1}(U)$, we get $(f \circ q)^{-1}(V) = (A \cap f^{-1}(U)) \cap f^{-1}(V)$ and so

$$\varphi((f \circ q)^{-1}(V)) = \varphi(A \cap f^{-1}(U)) \cap \varphi(f^{-1}(V)) ,$$

because φ is bijective. Since $p_U \circ \varphi = f$, we have that

$$\varphi(f^{-1}(V)) = \varphi((p_U \circ \varphi)^{-1}(V)) = \varphi(\varphi^{-1}(p_U^{-1}(V))) = p_U^{-1}(V) = V \times E .$$

So $\varphi((f \circ q)^{-1}(V)) = \varphi(A \cap f^{-1}(U)) \cap (V \times E) = V \times E'$. Then, restricting φ to $f^{-1}(V)$ we get a homeomorphism $\varphi : f^{-1}(V) \to V \times E'$. Notice that $E' \subseteq E$ is a finite discrete topological space. If we denote by $p_V : V \times E' \to V$ the projection on the first factor, we have that $p_V \circ \varphi : (f \circ q)^{-1}(V) \to V$ is the restriction to

$(f \circ q)^{-1}(V)$ of $p_U \circ \varphi = f$. This restriction is equal to $f \circ q$, by definition of q. So $p_V \circ \varphi = f \circ q$. This shows that $f \circ q : (f \circ q)^{-1}(V) \to V$ is a trivial covering. So $f \circ q : A \to X$ is a finite covering, i.e. an object of $\mathbf{Cov}_X$. It is clear that $q : A \to Y$ is a morphism of coverings from $f \circ q$ to f. Moreover, q is injective, so it is a monomorphism in $\mathbf{Cov}_X$ (see the proof of (G3) in the proposition 1.8). Since f is a connected object, we have that either $f \circ q$ is initial or q is an isomorphism of coverings. From the proof of (G2) in the proposition 1.8, it follows that the initial object in $\mathbf{Cov}_X$ is $\emptyset \to X$. Then $f \circ q$ is not initial, because we assumed $A \neq \emptyset$. So q is an isomorphism of coverings. In particular, it is bijective. So $A = \mathrm{Im}(q) = Y$. This proves that Y is a connected topological space.

2 The fundamental group of the pseudocircle

We start with the definition of the topological space we are interested in.

Definition 2.1. The *pseudocircle* is the topological space $X = \{0, 1, 2, 3\}$ with open subsets: $\emptyset$, $\{0\}$, $\{2\}$, $\{0, 2\}$, $\{0, 1, 2\}$, $\{0, 2, 3\}$, X.

Remark 2.2. First of all, the definition we gave in 2.1 gives indeed a topology: $\emptyset$ and X are open and it can be checked that the union and the intersection of any two open subsets are again open (since X is finite, there are finitely many open subsets, so any union of open subsets is a union of a finite family and to show tnat it is open we can apply induction after proving that the union of any two open subsets is open). Secondly, X is connected. To prove it, it is enough to check that for any open subset $U \notin \{\emptyset, X\}$ the complement $X \backslash U$ is not open. This is immediate from the definition.

Our aim is to compute $\hat{\pi}(X)$, where X is the pseudocircle. We will achieve this goal using a combinatorial approach: we will describe all finite coverings of X (this is possible because we are dealing with a very simple example: in general more sophisticated techniques are needed). Before doing this, we need to define the profinite completion of a group, because $\hat{\pi}(X)$ will turn out to be the profinite completion of a well-known group.

Lemma 2.3. *Let G be a group. We define*

$$I := \{N \trianglelefteq G \mid [G : N] < +\infty\} .$$

We consider on I the order relation defined by $N_1 \geq N_2$ if and only if $N_1 \subseteq N_2$. Then I is a directed partially ordered set. Moreover, for any $N_1, N_2 \in I$ such that $N_1 \geq N_2$, we define $f_{N_1 N_2} : G/N_1 \to G/N_2$, $\sigma N_1 \mapsto \sigma N_2$. Then $(G/N)_{N \in I}, (f_{N_1 N_2} : G/N_1 \to G/N_2)_{N_1, N_2 \in I,\, N_1 \geq N_2}$ is a projective system of finite groups.

Proof. It is clear that $\geq$ is an order relation. Let $N_1, N_2 \in I$, i.e. N_1 and N_2 are two normal subgroups of G of finite index, and consider $N_1 \cap N_2$. It is clear that $N_1 \cap N_2$ is again a normal subgroup. By the tower law for subgrups, we have that $[G : N_1 \cap N_2] = [G : N_1] \cdot [N_1 : N_1 \cap N_2]$. Moreover, by the second isomorphism theorem we have that $N_1/N_1 \cap N_2 \cong N_1 N_2/N_2$ and so $[N_1 : N_1 \cap N_2] = [N_1 N_2 : N_2] \leq$

$[G : N_2]$. Then $[G : N_1 \cap N_2] = [G : N_1] \cdot [N_1 : N_1 \cap N_2] \leq [G : N_1] \cdot [G : N_2] < +\infty$. So $N_1 \cap N_2 \in I$. We have that $N_1 \cap N_2 \subseteq N_1$ and $N_1 \cap N_2 \subseteq N_2$. So $N_1 \cap N_2 \geq N_1$ and $N_1 \cap N_2 \geq N_2$. This proves that I is directed.
It is clear that $f_{N_1 N_2}$ is a well-defined group homomorphism whenever $N_1 \subseteq N_2$, i.e. $N_1 \geq N_2$. If $N \in I$, we have that $f_{NN}(\sigma N) = \sigma N = \mathrm{id}_{G/N}(\sigma N)$ for any $\sigma N \in G/N$ and so $f_{NN} = \mathrm{id}_{G/N}$. Moreover, let $N_1, N_2, N_3 \in I$ such that $N_1 \geq N_2 \geq N_3$. Then $f_{N_1 N_3}(\sigma N_1) = \sigma N_3 = f_{N_2 N_3}(\sigma N_2) = f_{N_2 N_3}(f_{N_1 N_2}(\sigma N_1))$, for ever $\sigma N_1 \in G/N_1$. So $f_{N_1 N_3} = f_{N_2 N_3} \circ f_{N_1 N_2}$. Hence $(G/N)_{N \in I}, (f_{N_1 N_2} : G/N_1 \to G/N_2)_{N_1, N_2 \in I,\, N_1 \geq N_2}$ is a projective system of finite groups (the fact that the groups are finite follows from the definition of I). □

Definition 2.4. Let G be a group. The *profinite completion* of G, denoted by $\hat{G}$, is the projective limit $\varprojlim_{N \in I} G/N$ (which is a profinite group by definition), where the projective system $I, (G/N)_{N \in I}, (f_{N_1 N_2} : G/N_1 \to G/N_2)_{N_1, N_2 \in I,\, N_1 \geq N_2}$ is defined as in lemma 2.3.

Lemma 2.5. *Let G be a group. We denote by G-**sets** the category of fnite sets with an action of G (notice that in general G is not a topological group, so we cannot talk about continuity of an action of G; morphisms of G-sets are defined in the same way as we did for profinite groups). We have that G-**sets** is equivalent to the category $\hat{G}$-**sets** (since $\hat{G}$ is a profinite group, here we talk of continuous actions).*

Proof. We define a functor $F : \hat{G}$-**sets** $\to G$-**sets** as follows. Let E be a finite $\hat{G}$-set. Let $\sigma \in G$, $e \in E$. Consider $\widetilde{\sigma} = (\sigma N)_{N \in I} \in \prod_{N \in I} G/N$ (where I is defined as in lemma 2.3). For any $N_1, N_2 \in I$ with $N_1 \geq N_2$, we have that $f_{N_1 N_2}(\sigma N_1) = \sigma N_2$ by definition (see again lemma 2.3). So $\widetilde{\sigma} \in \varprojlim_{N \in I} G/N = \hat{G}$. Then we can define $\sigma.e := \widetilde{\sigma} e$. Let us check that this is a group action. If $\sigma = 1_G$, then $\widetilde{\sigma} = (1_G N)_{N \in I} = 1_{\hat{G}}$. Then $1_G.e = 1_{\hat{G}} e = e$. On the other hand, let $\sigma, \tau \in G$. Then $\widetilde{\sigma\tau} = ((\sigma\tau)N)_{N \in I} = ((\sigma N)(\tau N))_{N \in I} = (\sigma N)_{N \in I}(\tau N)_{N \in I} = \widetilde{\sigma}\widetilde{\tau}$. So

$$(\sigma\tau).e = \widetilde{\sigma\tau} e = (\widetilde{\sigma}\widetilde{\tau})e = \widetilde{\sigma}(\widetilde{\tau} e) = \sigma.(\widetilde{\tau} e) = \sigma.(\tau.e) \ ,$$

for any $e \in E$. So this indeed an action of G on E, which is then an object of G-**sets**. We define $F(E) = E$, equipped with this action. Let now E_1, E_2 be finite $\hat{G}$-sets with a morphism of $\hat{G}$-sets $f : E_1 \to E_2$. Let $\sigma \in G$, $e \in E_1$. Then

$$f(\sigma.e) = f(\widetilde{\sigma} e) = \widetilde{\sigma} f(e) = \sigma.f(e) \ .$$

So f is also a morphism of G-sets. Then we can define $F(f) = f$. For every finite $\hat{G}$-set E, we have that $F(\mathrm{id}_E) = \mathrm{id}_E = \mathrm{id}_{F(E)}$. Moreover, if E_1, E_2, E_3 are finite $\hat{G}$-sets with morphisms of $\hat{G}$-sets $f : E_1 \to E_2$ and $g : E_2 \to E_3$, then $F(g \circ f) = g \circ f = F(g) \circ F(f)$. So F is a functor.
We prove now that F is an equivalence of categories. By lemma 1.4.5, we have to prove that F is fully faithful and essentially surjective. Let E_1, E_2 be finite $\hat{G}$-sets with two morphisms $f, g : E_1 \to E_2$ such that $F(f) = F(g)$. This means that $f = F(f) = F(g) = g$. So F is faithful.
Let now E_1, E_2 be finite $\hat{G}$-sets and let $f : F(E_1) = E_1 \to F(E_2) = E_2$ be a morphism of G-sets. Let K be the kernel of the action of $\hat{G}$ on E_1, i.e. $K := \{\sigma \in$

$\hat{G} \mid \forall e \in E_1 \quad \sigma e = 1\} \leq \hat{G}$. Since E is fnite, by lemma 1.1.14 we have that K is open in $\hat{G}$. Then, since $1_{\hat{G}} \in K$, there exists an open neighbourhood of $1_{\hat{G}}$ that is contained in K. Recall that the topology on the projective limit is defined as the subspace topology of the product topology (considering the discrete topology on each factor). Then a local base for $\hat{G}$ at $1_{\hat{G}}$ is given by

$$\left\{ U_{N_1 \dots N_n} := \bigcap_{k=1}^{n} p_{N_k}^{-1}(\{1_G N_k\}) = \bigcap_{k=1}^{n} \operatorname{Ker}(p_{N_k}) \;\middle|\; n \in \mathbb{N},\ N_1, \dots, N_n \in I \right\} ,$$

where $p_N : \hat{G} \to G/N$ is the canonical projection (which is a continuous group homomorphism) for any $N \in I$. So there exist $n \in \mathbb{N}$, $N_1, \dots, N_n \in I$ such that $U_{N_1,\dots,N_n} \subseteq K$. Since I is directed, there exists $N_0 \in I$ such that $N_0 \geq N_k$ for any $k = 1, \dots, n$. If $\sigma = (\sigma_N N)_{N \in I} \in U_{N_0} = \operatorname{Ker}(p_{N_0})$, then $\sigma_{N_0} = p_{N_0}(\sigma) = 1_G N_0$ and $\sigma_{N_k} = f_{N_0 N_k}(\sigma_{N_0}) = f_{N_0 N_k}(1_G N_0) = 1_G N_k$ for any $k = 1, \dots, n$. So $\sigma \in \bigcap_{k=1}^{n} \operatorname{Ker}(p_{N_k}) = U_{N_1 \dots N_k}$. This shows that $U_{N_0} \subseteq U_{N_1 \dots N_n} \subseteq K$. Let now $\sigma = (\sigma_N N)_{N \in I} \in \hat{G}$. Consider $\widetilde{\sigma_{N_0}}^{-1} \sigma = (\sigma_{N_0} N)_{N \in I}^{-1} (\sigma_N N)_{N \in I} = ((\sigma_{N_0} N)^{-1} (\sigma_N N))_{N \in I} = ((\sigma_{N_0}^{-1} \sigma_N) N)_{N \in I}$. We have that $p_{N_0}(\widetilde{\sigma_{N_0}}^{-1} \sigma) = (\sigma_{N_0}^{-1} \sigma_{N_0}) N_0 = 1_G N_0$. So $\widetilde{\sigma_{N_0}}^{-1} \sigma \in \operatorname{Ker}(p_{N_0}) = U_{N_0} \subseteq K$. Then, for any $e \in E_1$, we have that $(\widetilde{\sigma_{N_0}}^{-1} \sigma) e = e$ and

$$\sigma e = (\widetilde{\sigma_{N_0}} \widetilde{\sigma_{N_0}}^{-1})(\sigma e) = \widetilde{\sigma_{N_0}}((\widetilde{\sigma_{N_0}}^{-1} \sigma) e) = \widetilde{\sigma_{N_0}} e = \sigma_{N_0} . e \ .$$

Since f is a morphism of G-sets, it follows that

$$f(\sigma e) = f(\sigma_{N_0} . e) = \sigma_{N_0} . f(e) = \sigma f(e)$$

for any $e \in E_1$. So f is a morphism of $\hat{G}$-sets. Moreover, $F(f) = f$ by definition of F. This proves that F is full.

Finally, let E be a finite set with an action of G. Let K be the kernel of the action of G on E, i.e. $K := \{\sigma \in G \mid \forall e \in E \quad \sigma e = e\}$. Then K is the kernel of the group homomorphism $\varphi : G \to \mathrm{S}_{E_1}$, $\sigma \mapsto (e \mapsto \sigma e)$. So K is a normal subgroup of G and, by the isomorphism theorem, $G/K \cong \operatorname{Im}(\varphi) \leq \mathrm{S}_{E_1}$. Then $[G : K] = |G/K| = |\operatorname{Im}(\varphi)| \leq |\mathrm{S}_{E_1}| < +\infty$. This proves that $K \in I$. For any $\sigma = (\sigma_N N)_{N \in I} \in \hat{G}$, $e \in E$, we define $\sigma e = \sigma_K e$. First of all, we have to check that this is well defined. If $\sigma_K K = \sigma'_K K$ (with $\sigma_K, \sigma'_K \in G$), then $\sigma_K^{-1} \sigma'_K \in K$. So, for any $e \in E$, we have that $(\sigma_K^{-1} \sigma'_K) e = e$, which implies that $\sigma'_K e = \sigma_K e$. We prove now that we have defined a group action. If $\sigma = 1_{\hat{G}}$, then $\sigma_K K = 1_G K$ and so $1_{\hat{G}} e = 1_G e = e$, for any $e \in E$. Moreover, let $\sigma = (\sigma_N N)_{N \in I}, \tau = (\tau_N N)_{N \in I} \in \hat{G}$. We have that $\sigma \tau = ((\sigma_N N)(\tau_N N))_{N \in I} = ((\sigma_N \tau_N) N)_{N \in I}$ and so

$$(\sigma \tau) e = (\sigma_K \tau_K) e = \sigma_K (\tau_K e) = \sigma (\tau_K e) = \sigma (\tau e) \ ,$$

for any $e \in E$. So we have indeed a group action. The kernel of this action is

$$\begin{aligned} \{\sigma = (\sigma_N N)_{N \in I} \in \hat{G} \mid \forall e \in E \quad \sigma_K e = \sigma e = e\} &= \\ = \{\sigma = (\sigma_N N)_{N \in I} \in \hat{G} \mid \sigma_K \in K\} &= \\ = \{\sigma = (\sigma_N N)_{N \in I} \in \hat{G} \mid p_K(\sigma) = \sigma_K K = K = 1_G K\} &= p_K^{-1}(\{1_G K\}) \ , \end{aligned}$$

which is open in $\hat{G}$ because $p_K : \hat{G} \to G/K$ is continuous and $\{1_G K\}$ is open in G/K (which has the discrete topology). Since E is finite, by lemma 1.1.14 we have that the action of $\hat{G}$ on E is continuous. So E, endowed with this action, is an object of $\hat{G}$-**sets**. We have that $F(E) = E$ as sets. Moreover, for any $\sigma \in G$, $e \in E$, we have that $\sigma.e = \widetilde{\sigma}e = (\sigma N)_{N \in I} e = \sigma e$. So the two actions of G on E coincide, i.e. $F(E) = E$ as objects of G-**sets**. Hence F is essentially surjective. □

Lemma 2.6. *Define a category* $\mathbf{D}$ *as follows: objects of* $\mathbf{D}$ *are pairs of the form* (E, σ)*, with* E *a finite set and* $\sigma \in \mathrm{S}_E$*, and a morphism from* (E_1, σ_1) *to* (E_2, σ_2) *is a map* $f : E_1 \to E_2$ *with* $\sigma_2 \circ f = f \circ \sigma_1$ *(the composition is defined in the obvious way). Then* $\mathbb{Z}$-**sets** *is equivalent to* $\mathbf{D}$.

Proof. For every object (E, σ) in $\mathbf{D}$ we have that $\sigma \circ \mathrm{id}_E = \sigma = \mathrm{id}_E \circ \sigma$ and so id_E is a morphism in $\mathbf{D}$. Moreover, let (E_1, σ_1), (E_2, σ_2), (E_3, σ_3) be objects of $\mathbf{D}$ with morphisms $f : (E_1, \sigma_1) \to (E_2, \sigma_2)$ and $g : (E_2, \sigma_2) \to (E_3, \sigma_3)$. Then $\sigma_2 \circ f = f \circ \sigma_1$ and $\sigma_3 \circ g = g \circ \sigma_2$. It follows that

$$\sigma_3 \circ (g \circ f) = (\sigma_3 \circ g) \circ f = (g \circ \sigma_2) \circ f = g \circ (\sigma_2 \circ f) = g \circ (f \circ \sigma_1) = (g \circ f) \circ \sigma_1 .$$

So $g \circ f$ is also a morphism in $\mathbf{D}$. This shows that $\mathbf{D}$ is indeed a category.
We define a functor $F : \mathbf{D} \to \mathbb{Z}$-**sets** as follows. Let (E, σ) be an element of $\mathbf{D}$. We define $z.e = \sigma^z(e)$ for every $z \in \mathbb{Z}$, $e \in E$. We have that $0.e = \sigma^0(e) = \mathrm{id}_E(e) = e$ for every $e \in E$. Moreover,

$$z_1.(z_2.e) = z_1.(\sigma^{z_2}(e)) = \sigma^{z_1}(\sigma^{z_2}(e)) = (\sigma^{z_1} \circ \sigma^{z_2})(e) = \sigma^{z_1 + z_2}(e) = (z_1 + z_2).e$$

for every $z_1, z_2 \in \mathbb{Z}$, $e \in E$. So we have defined an action of $\mathbb{Z}$ on E, which is then an object of $\mathbb{Z}$-**sets**. We define $F((E, \sigma)) = E$, equipped with this action. Let now $f : (E_1, \sigma_1) \to (E_2, \sigma_2)$ be a morphism in $\mathbf{D}$. By definition, $\sigma_2 \circ f = f \circ \sigma_1$. Then by induction we get $\sigma_2^z \circ f = f \circ \sigma_1^z$ for every $z \geq 0$. This implies $f \circ \sigma_1^{-z} = f \circ (\sigma_1^z)^{-1} = (\sigma_2^z)^{-1} \circ f = \sigma_2^{-z} \circ f$ for every $z \geq 0$. So $\sigma_2^z \circ f = f \circ \sigma_1^z$ for every $z \in \mathbb{Z}$. Then

$$f(z.e) = f(\sigma_1^z(e)) = (f \circ \sigma_1^z)(e) = (\sigma_2^z \circ f)(e) = \sigma_2^z(f(e)) = z.f(e)$$

for every $z \in \mathbb{Z}$, $e \in E_1$. So f is a morphism of $\mathbb{Z}$-sets. We define $F(f) = f$. For every object (E, σ) of $\mathbf{D}$, we have that $F(\mathrm{id}_E) = \mathrm{id}_E = \mathrm{id}_{F(E)}$. Moreover, if (E_1, σ_1), (E_2, σ_2), (E_3, σ_3) are objects of $\mathbf{D}$ with morphisms $f : (E_1, \sigma_1) \to (E_2, \sigma_2)$ and $g : (E_2, \sigma_2) \to (E_3, \sigma_3)$, then $F(g \circ f) = g \circ f = F(g) \circ F(f)$. So F is a functor.
We prove now that F is an equivalence of categories. By lemma 1.4.5, we have to prove that F is fully faithful and essentially surjective. Let (E_1, σ_1), (E_2, σ_2) be objects of $\mathbf{D}$ with two morphisms $f, g : (E_1, \sigma_1) \to (E_2, \sigma_2)$ such that $F(f) = F(g)$. This means that $f = F(f) = F(g) = g$. So F is faithful.
Let now (E_1, σ_1), (E_2, σ_2) be objects of $\mathbf{D}$ and let $f : F(E_1) = E_1 \to F(E_2) = E_2$ be a morphism of $\mathbb{Z}$-**sets**. For any $e \in E$, we have that

$$f(\sigma_1(e)) = f(\sigma_1^1(e)) = f(1.e) = 1.f(e) = \sigma_2^1(f(e)) = \sigma_2(f(e)) .$$

So $f \circ \sigma_1 = \sigma_2 \circ f$, i.e. f is also a morphism in $\mathbf{D}$. Since $F(f) = f$, F is full.
Finally, let E be a $\mathbb{Z}$-set. Define $\sigma : E \to E,\ e \mapsto 1e$. Then, by definition of action, σ

is invertible, with inverse $E \to E,\ e \mapsto (-1)e$. So (E, σ) is an object of $\mathbf{D}$. We have that $F((E, \sigma)) = E$ as sets, but we have to check that the two actions coincide. By definition, $1.e = \sigma(e) = 1e$ for any $e \in E$. Then by induction (using the definition of action) we get that $z.e = ze$ for every $z \geq 0$, $e \in E$. This implies that

$$(-z).e = (-z).(0e) = (-z).(z((-z)e)) = (-z).(z.((-z)e)) = 0.((-z)e) = (-z)e$$

for every $z \geq 0$, $e \in E$. Then $z.e = ze$ for any $z \in \mathbb{Z}$, $e \in E$, i.e. the two actions coincide. So $F((E, \sigma)) = E$ in $\mathbb{Z}$**-sets**. Hence F is essentially surjective. □

Corollary 2.7. *Let* $\mathbf{D}$ *be the category defined in lemma 2.6. Then* $\hat{\mathbb{Z}}$**-sets** *is equivalent to* $\mathbf{D}$.

Proof. It follows immediately from the lemmas 2.5 and 2.6. □

Proposition 2.8. *Let* X *be the pseudocircle (defined in 2.1). We have that* $\hat{\pi}(X) \cong \hat{\mathbb{Z}}$.

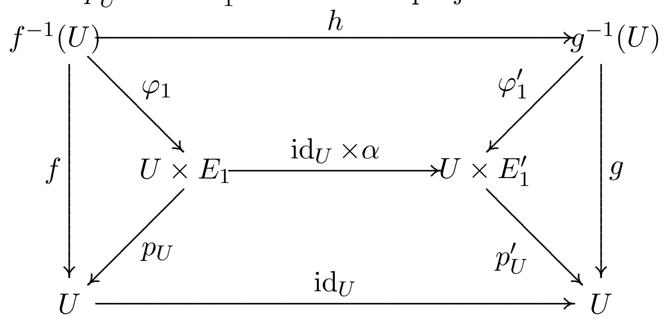
Proof. We have to show that $\mathbf{Cov}_X$ is equivalent to $\hat{\mathbb{Z}}$**-sets**, which by corollary 2.7 is equivalent to the category $\mathbf{D}$ defined in 2.6. So it is enough to prove that $\mathbf{Cov}_X$ is equivalent to $\mathbf{D}$.
We define a functor $F : \mathbf{Cov}_X \to \hat{\mathbb{Z}}$**-sets** as follows. Let $f : Y \to X$ be a finite covering of X. Then $f^{-1}(\{0\})$ is a finite set. Moreover, by definition of covering there exists an open subset U of X such that $1 \in U$ and the restriction $f : f^{-1}(U) \to U$ is a trivial covering. By definition of X, the only open subsets containing 1 are $\{0, 1, 2\}$ and X. But the restriction of a trivial covering is a trivial covering. So, if $f : f^{-1}(X) = Y \to X$ is a trivial covering, then also $f : f^{-1}(\{0, 1, 2\}) \to \{0, 1, 2\}$ is a trivial covering. So, in any case, we can choose $U = \{0, 1, 2\}$. Then there exist a discrete topological space E_1 and a homeomorphism $\varphi_1 : f^{-1}(U) \to U \times E_1$ such that $p_U \circ \varphi_1 = f$, where $p_U : U \times E_1 \to U$ is the projection on the first factor. Since $p_U \circ \varphi_1 = f$, we have that $f^{-1}(\{x\}) = \varphi_1^{-1}(p_U^{-1}(\{x\})) = \varphi_1^{-1}(\{x\} \times E_1)$ for any $x \in U = \{0, 1, 2\}$. Then $\varphi_1(f^{-1}(\{0\})) = \{0\} \times E_1$ and $\varphi_1(f^{-1}(\{2\})) = \{2\} \times E_1$ (we applied the fact that φ_1 is bijective), which allows us to restrict φ_1 to homeomorphisms $\varphi_1 : f^{-1}(\{0\}) \to \{0\} \times E_1$ and $\varphi_1 : f^{-1}(\{2\}) \to \{2\} \times E_1$. Analogously, by definition of covering there exists an open subset V of X such that $3 \in V$ and the restriction $f : f^{-1}(V) \to V$ is a trivial covering. We can choose $V = \{0, 2, 3\}$ because, by definition of X, the only open subsets containing 3 are $\{0, 2, 3\}$ and X. Then there exist a discrete topological space E_3 and a homeomorphism $\varphi_3 : f^{-1}(V) \to V \times E_3$ such that $p_V \circ \varphi_3 = f$, where $p_V : V \times E_3 \to V$ is the projection on the first factor. As above, we can restrict φ_3 to homeomorphisms $\varphi_3 : f^{-1}(\{0\}) \to \{0\} \times E_3$ and $\varphi_3 : f^{-1}(\{2\}) \to \{2\} \times E_3$. Define $i_{1,0} : E_1 \to \{0\} \times E_1,\ e \mapsto (0, e)$, $i_{1,2} : E_1 \to \{2\} \times E_1,\ e \mapsto (2, e)$, $i_{3,0} : E_3 \to \{0\} \times E_3,\ e \mapsto (0, e)$ and $i_{3,2} : E_3 \to \{2\} \times E_3,\ e \mapsto (2, e)$. These maps are clearly bijective. Consider now

$$\psi := i_{3,2}^{-1} \circ \varphi_3 \circ \varphi_1^{-1} \circ i_{1,2} : E_1 \to E_3\ ,$$

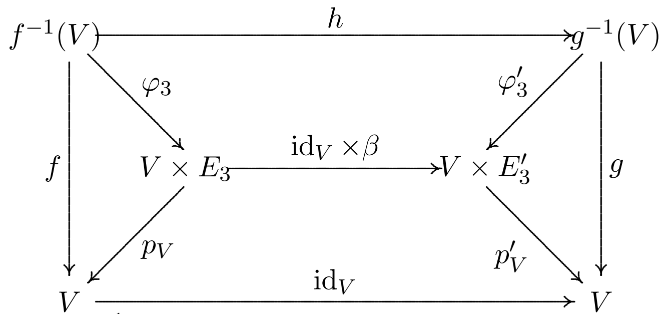
which is bijective because it is a composition of bijections. We have that ψ induces a bijection $\mathrm{id}_{\{0\}} \times \psi : \{0\} \times E_1 \to \{0\} \times E_3$. Define $\sigma := \varphi_3^{-1} \circ (\mathrm{id}_{\{0\}} \times \psi) \circ \varphi_1 :$

$f^{-1}(\{0\}) \to f^{-1}(\{0\})$. We have that σ is bijective, because it is a composition of bijections. So $(f^{-1}(\{0\}), \sigma)$ is an element of $\mathbf{D}$. We define $F(f) := (f^{-1}(\{0\}), \sigma)$ (for the sake of brevity, we omit to check that the definition of σ does not depend on the choice of the discrete topological spaces E_1', E_3' and of the homeomorphisms φ_1', φ_3').

Now we have to define F on morphisms. Let $f : Y \to X$, $g : Z \to X$ be finite coverings of X and let $h : Y \to Z$ be a morphism of coverings from f to g. As above, let $F(f) = (f^{-1}(\{0\}), \sigma)$, $F(g) = (g^{-1}(\{0\}), \sigma')$. Since h is a morphism of coverings, we have that $f = g \circ h$. Then $g(h(f^{-1}(\{0\})) = f(f^{-1}(\{0\})) \subseteq \{0\}$, which implies that $h(f^{-1}(\{0\})) \subseteq g^{-1}(\{0\})$. So we can restrict h and get a map $h : f^{-1}(\{0\}) \to g^{-1}(\{0\})$. We claim that this map is a morphism in $\mathbf{D}$ from $(f^{-1}(\{0\}), \sigma)$ to $(g^{-1}(\{0\}), \sigma')$. Let U, V, E_1, E_3, φ_1, φ_3, $i_{1,0}$, $i_{1,2}$, $i_{3,0}$, $i_{3,2}$ and ψ be as above. Moreover, we denote by E_1', E_3', φ_1', φ_3', $i_{1,0}'$, $i_{1,2}'$, $i_{3,0}'$, $i_{3,2}'$ and ψ' the topological spaces and the maps obtained in the same way, but starting from the finite covering g. Then $\sigma = \varphi_3^{-1} \circ (\mathrm{id}_{\{0\}} \times \psi) \circ \varphi_1$ and $\sigma' = (\varphi_3')^{-1} \circ (\mathrm{id}_{\{0\}} \times \psi') \circ \varphi_1'$. By lemma 1.5, there exists an open subset of X that contains 1 and above which f, g and h are trivial. Since the only open subsets containing 1 are U and X and triviality above X implies triviality above U, we have that f, g and h are trivial above U. Then there exists a map $\alpha : E_1 \to E_1'$ such that the following diagram is commutative, where $p_U : U \times E_1 \to U$ and $p_U' : U \times E_1' \to U$ are the projections on the first factor.



Analogously, by lemma 1.5, there exists an open subset of X that contains 3 and above which f, g and h are trivial. Since the only open subsets containing 3 are V and X and triviality above X implies triviality above V, we have that f, g and h are trivial above V. Then there exists a map $\beta : E_3 \to E_3'$ such that the following diagram is commutative, where $p_V : V \times E_3 \to V$ and $p_V' : V \times E_3' \to V$ are the projections on the first factor.



Now (restricting h to $f^{-1}(\{0\})$) we have that

$$\sigma' \circ h = (\varphi_3')^{-1} \circ (\mathrm{id}_{\{0\}} \times \psi') \circ \varphi_1' \circ h =$$

$$= (\varphi_3')^{-1} \circ (\mathrm{id}_{\{0\}} \times \psi') \circ (\mathrm{id}_U \times \alpha) \circ \varphi_1 = (\varphi_3')^{-1} \circ (\mathrm{id}_{\{0\}} \times (\psi' \circ \alpha)) \circ \varphi_1$$

and

$$\begin{aligned} h \circ \sigma = h \circ \varphi_3^{-1} \circ (\mathrm{id}_{\{0\}} \times \psi) \circ \varphi_1 = \\ = (\varphi_3')^{-1} \circ (\mathrm{id}_V \times \beta) \circ (\mathrm{id}_{\{0\}} \times \psi) \circ \varphi_1 = (\varphi_3')^{-1} \circ (\mathrm{id}_{\{0\}} \times (\beta \circ \psi)) \circ \varphi_1 \ . \end{aligned}$$

For any $e \in E_1$, we have that

$$i'_{1,2}(\alpha(e)) = (2, \alpha(e)) = (\mathrm{id}_{\{2\}} \times \alpha)((2, e)) = (\mathrm{id}_{\{2\}} \times \alpha)(i_{1,2}(e)) \ .$$

So $i'_{1,2} \circ \alpha = (\mathrm{id}_{\{2\}} \times \alpha) \circ i_{1,2}$. On the other hand, for any $e \in E_3$ we have that $i'_{3,2}(\beta(e)) = (2, \beta(e)) = (\mathrm{id}_{\{2\}} \times \beta)((2, e)) = (\mathrm{id}_{\{2\}} \times \beta)(i_{3,2}(e))$. So $i'_{3,2} \circ \beta = (\mathrm{id}_{\{2\}} \times \beta) \circ i_{3,2}$ and $\beta \circ i_{3,2}^{-1} = (i'_{3,2})^{-1} \circ (\mathrm{id}_{\{2\}} \times \beta)$. Then

$$\begin{aligned} \psi' \circ \alpha = (i'_{3,2})^{-1} \circ \varphi_3' \circ (\varphi_1')^{-1} \circ i'_{1,2} \circ \alpha = \\ = (i'_{3,2})^{-1} \circ \varphi_3' \circ (\varphi_1')^{-1} \circ (\mathrm{id}_{\{2\}} \times \alpha) \circ i_{1,2} = (i'_{3,2})^{-1} \circ \varphi_3' \circ h \circ \varphi_1^{-1} \circ i_{1,2} = \\ = (i'_{3,2})^{-1} \circ (\mathrm{id}_{\{2\}} \times \beta) \circ \varphi_3 \circ \varphi_1^{-1} \circ i_{1,2} = \beta \circ i_{3,2}^{-1} \circ \varphi_3 \circ \varphi_1^{-1} \circ i_{1,2} = \beta \circ \psi \ . \end{aligned}$$

So $\sigma' \circ h = (\varphi_3')^{-1} \circ (\mathrm{id}_{\{0\}} \times (\psi' \circ \alpha)) \circ \varphi_1 = (\varphi_3')^{-1} \circ (\mathrm{id}_{\{0\}} \times (\beta \circ \psi)) \circ \varphi_1 = h \circ \sigma$, i.e. $h : f^{-1}(\{0\}) \to g^{-1}(\{0\})$ is a morphism in **D** from $(f^{-1}(\{0\}), \sigma) = F(f)$ to $(g^{-1}(\{0\}), \sigma') = F(g)$. Then we can define $F(h) := h_{|_{f^{-1}(\{0\})}} : F(f) \to F(g)$.
For every finite covering $f : Y \to X$ we have that $F(\mathrm{id}_Y) = (\mathrm{id}_Y)_{|_{f^{-1}(\{0\})}} = \mathrm{id}_{f^{-1}(\{0\})} = \mathrm{id}_{F(f)}$. Moreover, if $f_1 : Y_1 \to X$, $f_2 : Y_2 \to X$ and $f_3 : Y_3 \to X$ are finite coverings of X with morphisms of coverings $h_1 : Y_1 \to Y_2$ and $h_2 : Y_2 \to Y_3$, we have that

$$F(h_2 \circ h_1) = (h_2 \circ h_1)_{|_{f^{-1}(\{0\})}} = (h_2)_{|_{g^{-1}(\{0\})}} \circ (h_1)_{|_{f^{-1}(\{0\})}} = F(h_2) \circ F(h_1) \ .$$

So F is a functor.
We prove now that F is an equivalence of categories. By lemma 1.4.5, we have to prove that F is fully faithful and essentially surjective. Let $f : Y \to X$, $g : Z \to X$ be finite coverings of X with two morphisms of coverings $h, h' : Y \to Z$ such that $F(h) = F(h')$. Let U, V, E_1, E_3, E_1', E_3', φ_1, φ_3, φ_1', φ_3', α and β be as above. Also, as above, we can find maps $\alpha' : E_1 \to E_1'$ and $\beta' : E_3 \to E_3'$ such that restricting h' to $f^{-1}(U)$ we have $\varphi_1' \circ h' = (\mathrm{id}_U \times \alpha') \circ \varphi_1$ and restricting h' to $f^{-1}(V)$ we have $\varphi_3' \circ h' = (\mathrm{id}_V \times \beta) \circ \varphi_3$. Since $h_{|_{f^{-1}(\{0\})}} F(h) = F(h') = (h')_{|_{f^{-1}(\{0\})}} F(h)$, restricting h and h' to $f^{-1}(\{0\})$ we have that

$$\mathrm{id}_{\{0\}} \times \alpha = \varphi_1' \circ h \circ \varphi_1^{-1} = \varphi_1' \circ h' \circ \varphi_1^{-1} = \mathrm{id}_{\{0\}} \times \alpha \ .$$

So $\alpha = \alpha'$, which implies that $h_{|_{f^{-1}(U)}} = (\varphi_1')^{-1} \circ (\mathrm{id}_U \times \alpha) \circ \varphi_1 = (\varphi_1')^{-1} \circ (\mathrm{id}_U \times \alpha') \circ \varphi_1 = (h')_{|_{f^{-1}(U)}}$. Now, restricting h and h' to $\{1, 3\}$, we have that

$$\mathrm{id}_{\{1,3\}} \times \beta = \varphi_3' \circ h \circ \varphi_3^{-1} = \varphi_3' \circ h' \circ \varphi_3^{-1} = \mathrm{id}_{\{1,3\}} \times \beta \ .$$

So $\beta = \beta'$, which implies that $h_{|_{f^{-1}(V)}} = (\varphi_3')^{-1} \circ (\mathrm{id}_V \times \beta) \circ \varphi_3 = (\varphi_3')^{-1} \circ (\mathrm{id}_V \times \beta') \circ \varphi_3 = (h')_{|_{f^{-1}(V)}}$. Since $X = U \cup V$, we have that $Y = f^{-1}(X) = f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$. So we must have $h = h'$. This proves that F is faithful.
Let now $f : Y \to X$, $g : Z \to X$ be finite coverings of X and consider a morphism $\chi : F(f) \to F(g)$ in $\mathbf{D}$. This means that $\chi : f^{-1}(\{0\}) \to g^{-1}(\{0\})$ is a map such that $\sigma' \circ \chi = \chi \circ \sigma$, where $F(f) = (f^{-1}(\{0\}), \sigma)$ and $F(g) = (g^{-1}(\{0\}), \sigma')$. Let U, V, E_1, E_3, E_1', E_3', φ_1, φ_3, φ_1', φ_3', $i_{1,0}$, $i_{1,2}$, $i_{3,0}$, $i_{3,2}$, $i_{1,0}'$, $i_{1,2}'$, $i_{3,0}'$, $i_{3,2}'$, ψ and ψ' be as above. Define $\alpha := (i_{1,0}')^{-1} \circ \varphi_1' \circ \chi \circ \varphi_1^{-1} \circ i_{1,0} : E_1 \to E_1'$ and $\beta := (i_{3,0}')^{-1} \circ \varphi_3' \circ \chi \circ \varphi_3^{-1} \circ i_{3,0} : E_3 \to E_3'$. Then α and β are continuous because E_1, E_1', E_3, E_3' are all discrete. Moreover, let $h_1 := (\varphi_1')^{-1} \circ (\mathrm{id}_U \times \alpha) \circ \varphi_1 : f^{-1}(U) \to g^{-1}(U) \subseteq Z$ and $h_3 := (\varphi_3')^{-1} \circ (\mathrm{id}_V \times \beta) \circ \varphi_3 : f^{-1}(V) \to g^{-1}(V) \subseteq Z$. Then h_1 and h_3 are both continuous, because they are compositions of continuous maps ($\mathrm{id}_U \times \alpha$ and $\mathrm{id}_V \times \beta$ are continuous because α and β are continuous). Moreover,

$$\begin{aligned}(\mathrm{id}_U \times \alpha)((0,e)) = (0, \alpha(e)) = i_{1,0}'(((i_{1,0}')^{-1} \circ \varphi_1' \circ \chi \circ \varphi_1^{-1} \circ i_{1,0})(e)) = \\ = (\varphi_1' \circ \chi \circ \varphi_1^{-1})(i_{1,0}(e)) = (\varphi_1' \circ \chi \circ \varphi_1^{-1})((0,e))\end{aligned}$$

for any $e \in E_1$. Since $\varphi_1(f^{-1}(\{0\})) = \{0\} \times E_1$ (see above), this implies that $(h_1)_{|_{f^{-1}(\{0\})}} = (\varphi_1')^{-1} \circ \varphi_1' \circ \chi \circ \varphi_1^{-1} \circ \varphi_1 = \chi$. Analogously, we have that

$$\begin{aligned}(\mathrm{id}_U \times \beta)((0,e)) = (0, \beta(e)) = i_{3,0}'(((i_{3,0}')^{-1} \circ \varphi_3' \circ \chi \circ \varphi_3^{-1} \circ i_{3,0})(e)) = \\ = (\varphi_3' \circ \chi \circ \varphi_3^{-1})(i_{3,0}(e)) = (\varphi_3' \circ \chi \circ \varphi_3^{-1})((0,e))\end{aligned}$$

for any $e \in E_3$ and, since $\varphi_3(f^{-1}(\{0\})) = \{0\} \times E_3$ (see above), this implies that $(h_3)_{|_{f^{-1}(\{0\})}} = (\varphi_3')^{-1} \circ \varphi_3' \circ \chi \circ \varphi_3^{-1} \circ \varphi_3 = \chi$. So $(h_1)_{|_{f^{-1}(\{0\})}} = (h_1)_{|_{f^{-1}(\{0\})}}$. On the other hand, we have that

$$\begin{aligned}(\mathrm{id}_U \times \alpha)((2,e)) = (2, \alpha(e)) = i_{1,2}'(((i_{1,0}')^{-1} \circ \varphi_1' \circ \chi \circ \varphi_1^{-1} \circ i_{1,0})(e)) = \\ = (i_{1,2}' \circ (i_{1,0}')^{-1} \circ \varphi_1' \circ \chi \circ \varphi_1^{-1} \circ i_{1,0} \circ i_{1,2}^{-1})((2,e))\end{aligned}$$

for any $e \in E_1$. Since $\varphi_1(f^{-1}(\{2\})) = \{2\} \times E_1$ (see above), this implies that $(h_1)_{|_{f^{-1}(\{2\})}} = (\varphi_1')^{-1} \circ i_{1,2}' \circ (i_{1,0}')^{-1} \circ \varphi_1' \circ \chi \circ \varphi_1^{-1} \circ i_{1,0} \circ i_{1,2}^{-1} \circ \varphi_1$. Analogously,

$$\begin{aligned}(\mathrm{id}_U \times \beta)((2,e)) = (2, \beta(e)) = i_{3,2}'(((i_{3,0}')^{-1} \circ \varphi_3' \circ \chi \circ \varphi_3^{-1} \circ i_{3,0})(e)) = \\ = (i_{3,2}' \circ (i_{3,0}')^{-1} \circ \varphi_3' \circ \chi \circ \varphi_3^{-1} \circ i_{3,0} \circ i_{3,2}^{-1})((2,e))\end{aligned}$$

for any $e \in E_3$ and, since $\varphi_3(f^{-1}(\{2\})) = \{2\} \times E_3$ (see above), this implies that $(h_3)_{|_{f^{-1}(\{2\})}} = (\varphi_3')^{-1} \circ i_{3,2}' \circ (i_{3,0}')^{-1} \circ \varphi_3' \circ \chi \circ \varphi_3^{-1} \circ i_{3,0} \circ i_{3,2}^{-1} \circ \varphi_3$. Recalling the definition of ψ, we have that

$$\begin{aligned}(\mathrm{id}_{\{0\}} \times \psi)((0,e)) = (0, \psi(e)) = i_{3,0}(\psi(e)) = i_{3,0}((i_{3,2}^{-1} \circ \varphi_3 \circ \varphi_1^{-1} \circ i_{1,2})(e)) = \\ = (i_{3,0} \circ i_{3,2}^{-1} \circ \varphi_3 \circ \varphi_1^{-1} \circ i_{1,2} \circ i_{1,0}^{-1})((0,e))\end{aligned}$$

for any $e \in E_1$. So $\mathrm{id}_{\{0\}} \times \psi = i_{3,0} \circ i_{3,2}^{-1} \circ \varphi_3 \circ \varphi_1^{-1} \circ i_{1,2} \circ i_{1,0}^{-1}$. Analogously, $\mathrm{id}_{\{0\}} \times \psi' = i'_{3,0} \circ (i'_{3,2})^{-1} \circ \varphi'_3 \circ (\varphi'_1)^{-1} \circ i'_{1,2} \circ (i'_{1,0})^{-1}$. Then

$$\begin{aligned}&(\varphi'_3)^{-1} \circ i'_{3,0} \circ (i'_{3,2})^{-1} \circ \varphi'_3 \circ (\varphi'_1)^{-1} \circ i'_{1,2} \circ (i'_{1,0})^{-1} \circ \varphi'_1 \circ \chi = \\ &\quad = (\varphi'_3)^{-1} \circ (\mathrm{id}_{\{0\}} \times \psi') \circ \varphi'_1 \circ \chi = \sigma' \circ \chi = \chi \circ \sigma = \chi \circ \varphi_3^{-1} \circ (\mathrm{id}_{\{0\}} \times \psi) \circ \varphi_1 = \\ &\qquad = \chi \circ \varphi_3^{-1} \circ i_{3,0} \circ i_{3,2}^{-1} \circ \varphi_3 \circ \varphi_1^{-1} \circ i_{1,2} \circ i_{1,0}^{-1} \circ \varphi_1 \,.\end{aligned}$$

This implies that

$$\begin{aligned}(h_1)_{|_{f^{-1}(\{2\})}} &= (\varphi'_1)^{-1} \circ i'_{1,2} \circ (i'_{1,0})^{-1} \circ \varphi'_1 \circ \chi \circ \varphi_1^{-1} \circ i_{1,0} \circ i_{1,2}^{-1} \circ \varphi_1 = \\ &= (\varphi'_3)^{-1} \circ i'_{3,2} \circ (i'_{3,0})^{-1} \circ \varphi'_3 \circ \chi \circ \varphi_3^{-1} \circ i_{3,0} \circ i_{3,2}^{-1} \circ \varphi_3 = (h_3)_{|_{f^{-1}(\{2\})}} \,.\end{aligned}$$

Then $(h_1)_{|_{f^{-1}(\{0\}) \cup f^{-1}(\{2\})}} = (h_3)_{|_{f^{-1}(\{0\}) \cup f^{-1}(\{2\})}}$. Since $f^{-1}(U) \cap f^{-1}(V) = f^{-1}(U \cap V) = f^{-1}(\{0,2\}) = f^{-1}(\{0\}) \cup f^{-1}(\{2\})$ and $f^{-1}(U) \cup f^{-1}(V) = f^{-1}(U \cup V) = f^{-1}(X) = Y$, we can glue h_1 and h_3 to get a continuous map $h : Y \to Z$. Recall that $p_U \circ \varphi_1 = f$ and $p'_U \circ \varphi'_1 = g$, where $p_U : U \times E_1 \to U$ and $p'_U : U \times E'_1 \to U$ are the projections on the first factors. Then

$$g \circ h_1 = g \circ (\varphi'_1)^{-1} \circ (\mathrm{id}_U \times \alpha) \circ \varphi_1 = p'_U \circ (\mathrm{id}_U \times \alpha) \circ \varphi_1 = \mathrm{id}_U \circ p_U \circ \varphi_1 = f \,.$$

Analogously, we have that $p_V \circ \varphi_3 = f$ and $p'_V \circ \varphi'_3 = g$, where $p_V : V \times E_3 \to V$ and $p'_V : V \times E'_3 \to V$ are the projections on the first factors, and so

$$g \circ h_3 = g \circ (\varphi'_3)^{-1} \circ (\mathrm{id}_V \times \beta) \circ \varphi_3 = p'_V \circ (\mathrm{id}_V \times \beta) \circ \varphi_3 = \mathrm{id}_V \circ p_V \circ \varphi_3 = f \,.$$

Then $g \circ h = f$. So h is a morphism of coverings from f to g. Moreover, $F(h) = h_{|_{f^{-1}(\{0\})}} = \chi$. This proves that F is full.
Finally, let (E, σ) be an object of $\mathbf{D}$. Consider the discrete topology on E and define $Y_1 := U \times E$ and $Y_3 := V \times E$, with the product topology. Moreover, consider the maps

$$\gamma_1 : \{0,2\} \times E \to Y_3,\ (x,e) \mapsto (x,e)$$

and

$$\gamma_3 : \{0,2\} \times E \to Y_3,\ (x,e) \mapsto \begin{cases}(x, \sigma^{-1}(e)) & \text{if } x = 0 \\ (x,e) & \text{if } x = 2\end{cases}$$

(recall that σ is bijective, by definition of $\mathbf{D}$). Notice that the subspace topology on $\{0,2\}$ is the discrete topology, so also the product $\{0,2\} \times E$ has the discrete topology, which implies that γ_1 and γ_3 are continuous. Moreover, γ_1 and γ_3 are both injective (for γ_3, this follow from the injectivity of σ^{-1}). Define on the disjoint union $Y_1 \amalg Y_3$ the following equivalence relation: given $y, y' \in Y_1 \amalg Y_3$, we say that $y \sim y'$ if and only if $y = y'$ or there exists a pair $(x,e) \in \{0,2\} \times E$ such that $y = \gamma_i((x,e))$ and $y' = \gamma_j((x,e))$, with $i,j \in \{1,3\}$ (it is immediate to check that this is an equivalence relation, using the fact that γ_1 and γ_3 are injective). Consider then the quotient space $Y := (Y_1 \amalg Y_3)/\sim$. Let $p_U : Y_1 = U \times E \to U \subseteq X$ and $p_V : Y_2 = V \times E \to V \subseteq X$ be the projections on the first factors, which are continuous by definition of product topology. Gluing them, we get a continuous map $p : Y_1 \amalg Y_3 \to X$. For any $(x, e) \in \{0, 2\} \times E$, we have that

$$p(\gamma_1((x,e))) = p_U(\gamma_1((x,e))) = p_U((x,e)) = x = \\ = p_U((x,\sigma^{-1}(e))) = p_U(\gamma_3((x,e))) = p(\gamma_3((x,e))) \; .$$

It follows that $p(y) = p(y')$ whenever $y, y' \in Y_1 \amalg Y_3$ are such that $y \sim y'$. Then, by the universal property of the quotient of topological spaces, we can factor p through a continuous map $f : Y = (Y_1 \amalg Y_3)/{\sim} \to X$ such that $p = f \circ \pi$, where $\pi : Y_1 \amalg Y_3 \to (Y_1 \amalg Y_3)/{\sim}$ is the canonical projection on the quotient. We claim that f is a finite covering. Since π is surjective, we have

$$f^{-1}(U) = \pi(\pi^{-1}(f^{-1}(U))) = \pi(p^{-1}(U)) = \pi(p_U^{-1}(U) \amalg p_V^{-1}(U)) = \\ = \pi(Y_1 \amalg ((U \cap V) \times E)) = \pi(Y_1) \cup \pi((U \cap V) \times E) \; .$$

For any $(x, e) \in (U \cap V) \times E = \{1, 2\} \times E \subseteq Y_3$, we have that $(x, e) = \gamma_3((x, \sigma(e)))$ and so $(x, e) \sim \gamma_1((x, \sigma(e))) = (x, \sigma(e))$, which implies that $\pi((x, e)) = \pi((x, \sigma(e))) \in \pi(Y_1)$. This shows that $\pi((U \cap V) \times E) \subseteq \pi(Y_1)$. So $f^{-1}(U) = \pi(Y_1) \cup \pi((U \cap V) \times E) = \pi(Y_1)$. We claim that the restriction $\pi_{|Y_1} : Y_1 \to \pi(Y_1) = f^{-1}(U)$ is a homeomorphism. Surjectivity and continuity are clear. If $y, y' \in Y_1$ are such that $\pi(y) = \pi(y')$, then $y \sim y'$. By definition of $\sim$, this means that $y = y'$ or there exist $(x, e) \in \{0, 2\} \times E$, $i, j \in \{1, 3\}$ such that $y = \gamma_i((x, e))$ and $y' = \gamma_j((x, e))$. In the last case, since $y, y' \in Y_1$, we must have $i = j = 1$ and so $y = \gamma_1((x, e)) = y'$. Then $\pi_{|Y_1}$ is injective. It remains to prove that $\pi_{|Y_1} : Y_1 \to \pi(Y_1)$ is open. By definition of product topology, it is enough to show that $\pi(W \times \{e\})$ is open for every $W \subseteq U$ open, $e \in E$. Fix such W and e. By definition of quotient topology, we have to show that $\pi^{-1}(\pi(W \times \{e\})) \subseteq Y_1 \amalg Y_3$ is open. We have that

$$\pi^{-1}(\pi(W \times \{e\})) = (\pi^{-1}(\pi(W \times \{e\})) \cap Y_1) \amalg (\pi^{-1}(\pi(W \times \{e\})) \cap Y_3) \; .$$

Since $\pi_{|Y_1}$ is injective, $\pi^{-1}(\pi(W \times \{e\})) \cap Y_1 = W \times \{e\}$, which is open in Y_1. On the other hand, let $y \in \pi^{-1}(\pi(W \times \{e\})) \cap Y_3$. Then there exists $y' \in W \times \{e\} \subseteq Y_1$ such that $\pi(y) = \pi(y')$. This means that $y \sim y'$. Since $y \in Y_3$ and $y' \in Y_1$, we cannot have $y = y'$. Then there exist $(x, e') \in \{0, 2\} \times E$, $i, j \in \{1, 3\}$ such that $y = \gamma_i((x, e'))$ and $y' = \gamma_j((x, e'))$. Since $y \in Y_3$ and $y' \in Y_1$, we must have $i = 3$ and $j = 1$. Then $(x, e') = \gamma_1((x, e')) = y' \in W \times \{e\}$, which means that $x \in W$ and $e' = e$. It follows that $y = \gamma_3((x, e)) \in \gamma_3((W \cap \{0, 2\}) \times \{e\})$. So $\pi^{-1}(\pi(W \times \{e\})) \cap Y_3 \subseteq \gamma_3((W \cap \{0, 2\}) \times \{e\})$. Conversely, if $x \in W \cap \{0, 2\}$, then $\gamma_3((x, e)) \sim \gamma_1((x, e)) = (x, e)$. So $\pi(\gamma_3((x, e))) = \pi((x, e)) \in \pi(W \times \{e\})$, which implies that $\gamma_3((x, e)) \in \pi^{-1}(\pi(W \times \{e\})) \cap Y_3$. Then

$$\pi^{-1}(\pi(W \times \{e\})) \cap Y_3 = \gamma_3((W \cap \{0,2\}) \times \{e\}) = \\ = \{\gamma_3((x,e)) \mid x \in W \cap \{0,2\}\} = \bigcup_{x \in W \cap \{0,2\}} \{\gamma_3((x,e))\} \; .$$

Let $x \in W \cap \{0, 2\}$. Then we have that either $x = 0$ or $x = 2$. If $x = 0$, then $\{\gamma_3((x, e))\} = \{(0, \sigma^{-1}(e))\} = \{0\} \times \{\sigma^{-1}(e)\}$. We have that $\{0\}$ is open in X and then also in V. Moreover, $\{\sigma^{-1}(e)\}$ is open in E (which is discrete). So $\{\gamma_3((x,e))\} = \{0\}\times\{\sigma^{-1}(e)\}$ is open in $V\times E = Y_3$. Analogously, one can show that, if $x = 2$, then $\{\gamma_3((x,e))\} = \{2\}\times\{e\}$ is open in $V\times E = Y_3$. It follows that $\pi^{-1}(\pi(W\times\{e\}))\cap Y_3 = \bigcup_{x\in W\cap\{0,2\}}\{\gamma_3((x,e))\}$ is open in Y_3. Then $\pi^{-1}(\pi(W\times\{e\})) = (\pi^{-1}(\pi(W\times\{e\}))\cap Y_1)\amalg(\pi^{-1}(\pi(W\times\{e\}))\cap Y_3)$ is open in $Y_1\amalg Y_3$. This proves that $\pi_{|Y_1}$ is open. So $\pi_{|Y_1} : Y_1 \to f^{-1}(U)$ is a homeomorphism. Then its inverse $\pi_{|Y_1}^{-1} : f^{-1}(U) \to Y_1 = U\times E$ is also a homeomorphism. By definition of f and p, we have that $f\circ\pi_{|Y_1} = p_{|Y_1} = p_U$ and so $p_U\circ\pi_{|Y_1}^{-1} = f$. This shows that $f : f^{-1}(U) \to U$ is a trivial covering. Analogously, one can show that $f^{-1}(V) = \pi(Y_3)$ and that $\pi_{|Y_3} : Y_3 \to \pi(Y_3)$ is a homeomorphism with $p_V\circ\pi_{|Y_3}^{-1} = f$. So $f : f^{-1}(V)\to V$ is a trivial covering. Then, since $X = U\cup V$, we have that f is a covering. Moreover, $f^{-1}(\{x\}) = (p_U\circ\pi_{|Y_1}^{-1})^{-1}(\{x\}) = \pi_{|Y_1}(p_U^{-1}(\{x\})) = \pi_{|Y_1}(\{x\}\times E) \cong \{x\}\times E$ for any $x\in U$ and $f^{-1}(\{x\}) = (p_V\circ\pi_{|Y_3}^{-1})^{-1}(\{x\}) = \pi_{|Y_3}(p_V^{-1}(\{x\})) = \pi_{|Y_3}(\{x\}\times E) \cong \{x\}\times E$ for any $x\in V$. In any case, $f^{-1}(\{x\})$ is finite. So f is a finite covering of X.

Consider now $F(f) = (f^{-1}(\{0\}),\tau)$. We have that $f^{-1}(\{0\}) = \pi_{|Y_1}(\{0\}\times E) = \pi_{|Y_3}(\{0\}\times E)$. Since $\pi_{|Y_1} : Y_1\to\pi(Y_1)$ is a homeomorphism, restricting to $\{0\}\times E$ we get a homeomorphism (in particular, a bijection) $\pi_{|Y_1} : \{0\}\times E\to\pi_{|Y_1}(\{0\}\times E) = f^{-1}(\{0\})$. Moreover, we have a bijection $i_0 : E\to\{0\}\times E,\ e\mapsto(0,e)$. Define $\varphi := \pi_{|Y_1}\circ i_0 : E\to f^{-1}(\{0\})$. Let also $i_2 : E\to\{2\}\times E,\ e\mapsto(2,e)$ and $\psi = i_2^{-1}\circ(\pi_{|Y_3})^{-1}\circ\pi_{|Y_1}\circ i_2 : E\to E$ (this definition makes sense because $\pi_{|Y_1}(\{2\}\times E) = f^{-1}(\{2\}) = \pi_{|Y_3}(\{2\}\times E)$). By definition of F, we have that $\tau = \pi_{|Y_3}\circ(\mathrm{id}_{\{0\}}\times\psi)\circ(\pi_{|Y_1})^{-1} : f^{-1}(\{0\})\to f^{-1}(\{0\})$ (see the construction above). For any $e\in E$, we have that

$$\pi_{|Y_1}(i_2(e)) = \pi_{|Y_1}((2,e)) = \pi(\gamma_1((2,e))) = \pi(\gamma_3((2,e))) = \pi_{|Y_3}((2,e)) = \pi_{|Y_3}(i_2(e))\ ,$$

because $\gamma_1((2,e))\sim\gamma_3((2,e))$. Then $\pi_{|Y_1}\circ i_2 = \pi_{|Y_3}\circ i_2$, which implies that $\psi = i_2^{-1}\circ(\pi_{|Y_3})^{-1}\circ\pi_{|Y_1}\circ i_2 = \mathrm{id}_E$. So $\tau = \pi_{|Y_3}\circ(\mathrm{id}_{\{0\}}\times\mathrm{id}_E)\circ(\pi_{|Y_1})^{-1} = \pi_{|Y_3}\circ\mathrm{id}_{\{0\}\times E}\circ(\pi_{|Y_1})^{-1} = \pi_{|Y_3}\circ(\pi_{|Y_1})^{-1}$. Moreover, for any $e\in E$ we have that

$$\begin{aligned}\pi_{|Y_3}(i_0(e)) = \pi_{|Y_3}((0,e)) = \pi(\gamma_3((0,\sigma(e)))) = \\ = \pi(\gamma_1((0,\sigma(e)))) = \pi_{|Y_1}((0,\sigma(e))) = \pi_{|Y_1}(i_0(\sigma(e)))\ ,\end{aligned}$$

because $\gamma_1((0,\sigma(e)))\sim\gamma_3((0,\sigma(e)))$. Then $\pi_{|Y_3}\circ i_0 = \pi_{|Y_1}\circ i_0\circ\sigma$. So

$$\tau\circ\varphi = \pi_{|Y_3}\circ(\pi_{|Y_1})^{-1}\circ\pi_{|Y_1}\circ i_0 = \pi_{|Y_3}\circ i_0 = \pi_{|Y_1}\circ i_0\circ\sigma = \varphi\circ\sigma\ ,$$

which implies also that $\varphi^{-1}\circ\tau = \sigma\circ\varphi^{-1}$. Then φ and φ^{-1} are morphisms in $\mathbf{D}$. So φ is an isomorphism in $\mathbf{D}$ from (E,σ) to $(f^{-1}(\{0\}),\tau) = F(f)$. Hence $F(f)\cong(E,\sigma)$ and so F is essentially surjective. □

Bibliography

[1] Henrik W. Lenstra. *Galois theory for schemes*. 1985. URL: `http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf`.

[2] Alexandre Grothendieck. *Revêtement étales et groupe fondamental (SGA1)*. Lecture Notes in Mathematics 224. Springer-Verlag, 1971.

[3] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Company, Reading, 1969.

[4] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, 1977.

[5] Ravi Vakil. *The Rising Sea: Foundations of Algebraic Geometry*. 2017. URL: `http://math.stanford.edu/~vakil/216blog/FOtopAGfeb0717public.pdf`.

[6] Angelo Vistoli. "Notes on Grothendieck topologies, fibered categories and descent theory". In: *arXiv preprint math/0412512* (2004).

[7] Michael Barr. "Abstract Galois theory". In: *Journal of Pure and Applied Algebra* 19 (1980), pp. 21–42.

[8] Hyman Bass. "Big projective modules are free". In: *Illinois Journal of Mathematics* 7 (1963), pp. 24–31.

[9] Hyman Bass. *Algebraic K-theory*. Benjamin, 1968.

[10] John William Scott Cassels and Albrecht Frölich. *Algebraic number theory: proceedings of an instructional conference*. Academic Press, 1967.

[11] F. De Meyer and E. Ingraham. *Separable algebras over commutative rings*. Lecture Notes in Mathematics 181. Springer-Verlag, Berlin, 1971.

[12] Claude Godbillon. *Eléments de topologie algébrique*. Hermann, Paris, 1971.

[13] Philip J. Higgins. *Notes on categories and groupoids*. Van Nostrand Reinhold, 1971.

[14] P. T. Johnstone. *Topos theory*. Academic Press, 1977.

[15] Irving Kaplansky. "Projective modules". In: *Annals of Mathematics* 68 (1958).

[16] Irving Kaplansky. *Fields and rings*. University of Chicago Press, 1972.

[17] T. Y. Lam. *Serre's conjecture*. Lecture Notes in Mathematics 635. Springer-Verlag, 1978.

[18] Serge Lang. *Algebraic number theory*. Addison-Wesley, 1970.

[19] Andy R. Magid. *The separable Galois theory of commutative rings*. Marcel Dekker, New York, 1974.

[20] William S. Massey. *Algebraic topology: an introduction.* Springer-Verlag, New York, 1977.

[21] James S. Milne. *Étale cohomology.* Princeton University Press, 1980.

[22] Elias Milnor. *Introduction to algebraic K-theory.* Princeton University Press, 1971.

[23] Jacob P. Murre. *Lectures on an introduction to Grothendieck's theory of the fundamental group.* Tata Institute of Fundamental Research Bombay, 1967.

[24] Jean-Pierre Serre. *Cohomologie galoisienne.* Lecture Notes in Mathematics. 5. Springer-Verlag, Berlin, 1973.

[25] Jean-Pierre Serre. *Arbres, amalgames, SL2.* Astérisque. Société mathématique de France, Paris, 1977.

[26] Edwin Weiss. *Algebraic number theory.* McGraw-Hill, New York, 1963.