Concordia University
Universitat Politècnica de Catalunya

Degree in Mathematics - Degree in Engineering Physics
Bachelor's Degree Thesis

Galois Theory for Schemes

Oriol Velasco Falguera

Supervisor (Concordia University): Adrian Iovita

Supervisor (UPC): Víctor Rotger Cerdà

May 2021

UNIVERSITÉ
Concordia
UNIVERSITY

UPC
UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Centre de Formació Interdisciplinària Superior

UPC
UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

UPC
UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona

telecos
BCN

I am deeply grateful to Professor Adrian Iovita. He has been extremely generous with his time as well as patient when giving me advice about the project. He has suggested a very stimulating topic on which I've loved to work. He has always provided the help that I needed, and dedicated a lot of time and effort to make sure that I was making progress on my learning process. It has been a real pleasure to be able to work on my undergraduate thesis under his supervision.

I would also like to express my sincere gratitude to Francesc Gispert, who has always been available to answer any doubt that I had during these months, and provided fast and very detailed answers. I also have to thank Francesc for reading all the answers to Hartshorne's exercises that I wrote when I was learning about schemes, and for giving me concrete corrections and hints.

I would like to extend my sincere thanks to all the people of the Number Theory group in Montréal, for letting me attend seminars and have lunch with them, and for introducing me to this beautiful subject. Finally, I am also very grateful to Victor Rotger and CFIS institution for providing the opportunity to work on my undergraduate thesis abroad in such a motivating environment.

Abstract

This thesis presents the construction of the étale fundamental group of a connected scheme. We prove that given a connected scheme X, there exists a profinite group $\pi(X)$, uniquely determined up to isomorphism, such that the category of finite étale coverings of X is equivalent to the category of finite sets with a continuous action of $\pi(X)$. The profinite group mentioned in this theorem is what we call the étale fundamental group. We will also prove that it is a generalization of the Galois group to the scheme-theoretic setting.

We start by introducing the formalism of Galois Categories, that characterizes axiomatically all the categories that are equivalent to the category of finite sets with a continuous action of a certain profinite group. This allows us to reduce the proof to checking that the category of finite étale coverings of a connected scheme satisfies this set of axioms. Then we study the category of finite étale coverings, first from an affine perspective through the concept of projective separable algebras and then in the general case. We introduce the concept of totally split morphisms, which simplifies the treatment of finite étale morphisms, and allows us to prove the theorem. At the end we give an explicit description of the étale fundamental group in the case of a locally noetherian normal integral scheme of dimension one.

Resum

En aquest treball presentem la construcció del grup fonamental étale per esquemes connexos. Demostrem que, donat un esquema connex X, existeix un grup profinit $\pi(X)$, únic llevat d'isomorfisme, tal que la categoria de recobriments finits étales de X és equivalent a la categoria de conjunts finits amb una acció contínua de $\pi(X)$. El grup profinit esmentat és el que anomenem grup fonamental étale. També demostrem que aquest grup és una generalització del grup de Galois per a esquemes connexos.

Comencem introduint el formalisme de Categories de Galois, que catacteritza de manera axiomàtica les categories que són equivalents a la categoria de conjunts finits amb una acció contínua d'un cert grup profinit. Això ens permet reduir la demostració a una verificació dels axiomes. A continuació estudiem la categoria de recobriments finits étales, en primer lloc des del punt de vista afí a través del concepte d'àlgebres projectives separables, i després en el cas general. Introduïm el concepte de morfismes totalment descomposats, que simplifica el tractament dels morfisimes finits étales i ens permet demostrar el teorema. Finalment, donem una descripció explícita del grup fonamental étale pel cas d'un esquema normal, íntegre i localment noetherià de dimensió u.

Resumen

En este trabajo presentamos la construcción del grupo fundamental étale para esquemas conexos. Demostramos que, dado un esquema conexo X, existe un grupo profinito $\pi(X)$, único salvo isomorfismo, tal que la categoría de recubrimientos finitos étales de X es equivalente a la categoría de conjuntos finitos con una acción continua del grupo $\pi(X)$. Este grupo $\pi(X)$ es el que denominamos grupo fundamental étale. También demostramos que dicho grupo es una generalización del Grupo de Galois en el contexto de los esquemas conexos.

Empezamos introduciendo el formalismo de las Categorías de Galois, que caracteriza de forma axiomática todas aquellas categorías que son equivalentes a la categoría de conjuntos finitos con una acción continua de un cierto grupo profinito. Esto nos permite reducir la demostración a una verificación de los axiomas. A continuación, estudiamos la categoría de recubrimientos finitos étales, en primer lugar desde un punto de vista afín, y luego de forma general. Introducimos el concepto de morfismos totalmente descompuestos, que simplifica el tratamiento de los morfismos finitos étales y permite probar el teorema. Finalmente, damos una descripción explícita del grupo fundamental étale para el caso de un esquema íntegro, normal y localmente noetheriano de dimensión uno.

Keywords

étale fundamental group, finite étale, Galois categories, schemes, algebraic geometry, number theory

Paraules clau

grup fonamental étale, finit étale, Categories de Galois, esquemes, geometria algebraica, teoria de nombres

Palabras clave

grupo fundamental étale, finito étale, Categorías de Galois, esquemas, geometría algebraica, teoría de números

MSC2020: 14G32

Contents

Introduction

This thesis is an study of the construction of the étale fundamental group of a connected scheme. Roughly speaking, given a connected scheme X we will assign to it a profinite group $\pi(X)$ that totally characterizes the *finite étale coverings of* X, that is, the set of finite étale morphisms of schemes with target X. To give a precise definition of finite étale morphisms of schemes, we need to introduce the concept of free separable algebras.

Definition. Let A be a ring, B an A-algebra that is free and finitely generated as an A-module. For every $b \in B$ we can define an A-linear map $m_b : B \to B$ by $m_b(x) = bx$. Denoting by $\mathrm{Tr}_{B/A}(b)$ the trace of this morphism, this defines an A-linear map $\mathrm{Tr}_{B/A} : B \to A$. Then, we say that B is a *free separable* A-algebra if the A-linear map

$$\begin{aligned} \varphi : B &\longrightarrow \mathrm{Mor}_A(B, A) \\ b &\longmapsto \quad \varphi(b) : B \longrightarrow A \\ &\qquad\qquad\qquad x \longmapsto (\varphi(b))(x) = \mathrm{Tr}(bx) \end{aligned}$$

is an isomorphism of A-modules.

Definition. A morphism of schemes $f : Y \to X$ is called *finite étale* if there exists a covering of X by open affine subsets $U_i = \mathrm{Spec}(A_i)$ such that $f^{-1}(U_i) = \mathrm{Spec}(B_i)$, where B_i is a free separable A_i-algebra.

Given a scheme X, we define the category of *finite étale coverings of* X as follows:

- **Objects**: Finite étale morphisms of schemes with target X.
- **Morphisms**: Given two objects $f : Y \to X$ and $g : Y' \to X$, a morphism from f to g is a morphism of schemes $h : Y \to Y'$ satisfying $f = gh$, i.e. making commutative the diagram $$\begin{tikzcd} Y \arrow[r, "h"] \arrow[d, "f"] & Y' \arrow[dl, "g"] \\ X & \end{tikzcd}$$

Then, the assignation $X \mapsto \pi(X)$ arises from the proof of the following theorem:

Theorem. *Let X be a connected scheme. Then there exists a unique profinite group π, uniquely determined up to isomorphism, such that the category of finite étale coverings of X is equivalent to the category of finite sets on which π acts continuously.*

The underlying idea is analogous to the procedure of Galois Theory for fields, where for a given field K, one builds a profinite group -the absolute Galois group of K- which totally characterizes the separable extensions of K. Moreover, it will be seen in Section 2.7 that this is more than an analogy, and that the theory of the étale fundamental groups of connected schemes generalizes the classical Galois Theory for fields.

After an introductory section with some background (Section 1), in Section 2 we introduce Grothendieck's formalism of Galois Categories, which characterizes axiomatically the categories that are equivalent to the category of finite sets on which π acts continuously, for some profinite group π. Then the statement of the theorem reduces to verifying that the finite étale coverings of X form a category which satisfies Grothendieck's axioms. Sections 3 and 4 are dedicated to the study of finite étale coverings: Section

3 deals with the affine algebraic setting of finite étale morphisms, and in Section 4 this information is translated to the scheme-theoretic setting and we prove the theorem.

We will expose the theory behind the construction of the étale fundamental group given by Lenstra in [5]. Therefore, the proofs of the auxiliary results that are left for the reader in [5] are the only original part of this thesis. We assume some basic background from commutative algebra ([1]) and scheme theory ([3], Chapter II, Sections 1-5). However, whenever we use results from these books, the particular result will be pointed out. Sometimes we will use results that are stated but not proved in [3] or [1]. When this happens, a proof can be found in Appendix A.2.

1. Background knowledge

1.1 Categories

This section contains a very basic introduction to Category Theory, based on [4]. We also give the definitions of some objects that are involved in the axioms of Galois Categories, which are needed in Section 2.

Definition 1.1. A *category*[1] $\mathbf{C}$ consists of

1. A set of *objects*, denoted $Ob(\mathbf{C})$,
2. $\forall A, B \in Ob(\mathbf{C})$, a set of *morphisms*, denoted $\mathrm{Mor}_{\mathbf{C}}(A, B)$
3. $\forall A, B, C \in Ob(\mathbf{C})$, a map

$$\mathrm{Mor}_{\mathbf{C}}(A, B) \times \mathrm{Mor}_{\mathbf{C}}(B, C) \to \mathrm{Mor}_{\mathbf{C}}(A, C)$$

which is denoted $(f, g) \mapsto g \circ f$, and is called the *composition* of g with f.

Satisfying that following properties:

1. The composition is an associative operation, that is, given $f \in \mathrm{Mor}_{\mathbf{C}}(A, B)$, $g \in \mathrm{Mor}_{\mathbf{C}}(B, C)$, $h \in \mathrm{Mor}_{\mathbf{C}}(C, D)$ we have $h \circ (g \circ f) = (h \circ g) \circ f$.
2. $\forall A \in Ob(\mathbf{C})$, $\exists \mathrm{id}_A \in \mathrm{Mor}_{\mathbf{C}}(A, A)$ satisfying that $\forall B \in Ob(\mathbf{C})$ and $f \in \mathrm{Mor}_{\mathbf{C}}(A, B)$, $f \circ \mathrm{id}_A = f$ and $\forall f \in \mathrm{Mor}_{\mathbf{C}}(B, A)$, $\mathrm{id}_A \circ f = f$.

A morphism $f \in \mathrm{Mor}_{\mathbf{C}}(A, B)$ is usually denoted as an arrow $f : A \to B$. We say that $f : A \to B$ is an *isomorphism* if it has an inverse: There exists $g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. The set of *automorphisms* of A, denoted $\mathrm{Aut}_{\mathbf{C}}(A)$ is the set of invertible elements of $\mathrm{Mor}_{\mathbf{C}}(A, A)$, and is a group under composition.

Definition 1.2. Let $\mathbf{C}$ be a category. The *opposite category* to $\mathbf{C}$, denoted $\mathbf{C}^{op}$, is the category whose set of objects is $Ob(\mathbf{C}^{op}) = Ob(\mathbf{C})$, and for any two objects $A, B \in Ob(\mathbf{C}^{op})$, its set of morphisms is $\mathrm{Mor}_{\mathbf{C}^{op}}(A, B) = \mathrm{Mor}_{\mathbf{C}}(B, A)$.

Let $\mathbf{C}$, $\mathbf{C}'$ be two categories.

Definition 1.3. A *functor* from $\mathbf{C}$ to $\mathbf{C}'$ consists of

1. A map $F : Ob(\mathbf{C}) \to Ob(\mathbf{C}')$,
2. $\forall A, B \in Ob(\mathbf{C})$, a map $F : \mathrm{Mor}_{\mathbf{C}}(A, B) \to \mathrm{Mor}_{\mathbf{C}'}(F(A), F(B))$ satisfying
   (a) $\forall A \in Ob(\mathbf{C})$, $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$
   (b) $\forall A, B, C \in Ob(\mathbf{C})$, and $f : A \to B$, $g : B \to C$, $F(g \circ f) = F(g) \circ F(f)$

A *contravariant functor* from $\mathbf{C}$ to $\mathbf{C}'$ is a functor from $\mathbf{C}^{op}$ to $\mathbf{C}'$.

Definition 1.4. Let $F, G : \mathbf{C} \to \mathbf{C}'$ be two functors. A morphism of functors $\sigma : F \to G$ is a set of morphisms $(\sigma_A)_{A \in Ob(\mathbf{C})}$, $\sigma_A : F(A) \to G(A)$ such that for every $f : A \to B$ the following diagram is

[1] In fact, this is the definition of a small category. In general, the objects of a category can form a class (a collection which is "bigger" than a set). The difference is subtle and comes from set theory. As we will see, we are only interested in small categories. Therefore, we will specify it when we require a category to be small, but we will not give a detailed treatment of this distinction.

commutative:

$$\begin{tikzcd} F(A) \arrow[r, "F(f)"] \arrow[d, "\sigma_A"] & F(B) \arrow[d, "\sigma_B"] \\ G(A) \arrow[r, "G(f)"] & G(B) \end{tikzcd}$$

Remark 1.1. Given two categories $\mathbf{C}, \mathbf{C}'$, the functors from $\mathbf{C}$ to $\mathbf{C}'$ form a category, where the objects are functors and the morphisms are morphisms of functors. This allows us to speak about isomorphisms between functors and automorphisms of functors.

Definition 1.5. A functor $F : \mathbf{C} \to \mathbf{C}'$ is an *equivalence of categories* if $\exists G : \mathbf{C}' \to \mathbf{C}$ and isomorphisms of functors $\sigma : G \circ F \to \mathrm{id}_{\mathbf{C}}$ and $\epsilon : F \circ G \to \mathrm{id}_{\mathbf{C}'}$. If an equivalence of categories exists between $\mathbf{C}$ and $\mathbf{C}'$ we say that $\mathbf{C}$ and $\mathbf{C}'$ are *equivalent*.

If a contravariant functor $F : \mathbf{C} \to \mathbf{C}'$ is an equivalence of categories, we say that it is an *antiequivalence of categories*, and that $\mathbf{C}$ and $\mathbf{C}'$ are *antiequivalent*.

Proposition 1.1. *$F : \mathbf{C} \to \mathbf{C}'$ is an equivalence of categories if and only if the two following conditions are satisfied:*

i) *Every object in $\mathbf{C}'$ is isomorphic to one of the form $F(A)$, for a certain $A \in \mathbf{C}$.*
ii) *For any $A, B \in Ob(\mathbf{C})$, F induces a bijective map $\mathrm{Mor}_{\mathbf{C}}(A, B) \to \mathrm{Mor}_{\mathbf{C}'}(F(A), F(B))$.*

Proof. $\boxed{\Rightarrow}$ Let $F : \mathbf{C} \to \mathbf{C}'$ and $G : \mathbf{C}' \to \mathbf{C}$ be the functors of the equivalence of categories. Let $X, Y \in Ob(\mathbf{C}')$, $A, B \in Ob(\mathbf{C})$. Then $\exists$ isomorphisms of functors σ, ϵ that make commutative the following diagrams, $\forall f : A \to B$ and $\forall g : X \to Y$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\sigma_A"] & B \arrow[d, "\sigma_B"] & X \arrow[r, "g"] \arrow[d, "\epsilon_X"] & Y \arrow[d, "\epsilon_Y"] \\ GF(A) \arrow[r, "GF(f)"] & GF(B) & FG(X) \arrow[r, "FG(g)"] & FG(Y) \end{tikzcd}$$

First note that $X \cong FG(X)$, so (i) is satisfied by taking $A = G(X)$.

Now let's proceed to prove (ii). Suppose that we have $F(f_1) = F(f_2)$. Then, $f_1 = \sigma_B^{-1} GF(f_1)\sigma_A = \sigma_B^{-1} GF(f_2)\sigma_A = f_2$. This proves that the map $F : \mathrm{Mor}_{\mathbf{C}}(A, B) \to \mathrm{Mor}_{\mathbf{C}'}(F(A), F(B))$ is injective. The same reasoning shows that G yields an injective map $G : \mathrm{Mor}_{\mathbf{C}}(F(A), F(B)) \to \mathrm{Mor}_{\mathbf{C}'}(GF(A), GF(B))$. Moreover, the map $\mathrm{Mor}_{\mathbf{C}}(A, B) \to \mathrm{Mor}_{\mathbf{C}'}(GF(A), GF(B))$, $f \mapsto GF(f)$ is bijective, and in particular injective.

Then let $g \in \mathrm{Mor}_{\mathbf{C}'}(F(A), F(B))$ and $f := \sigma_B^{-1} G(g)\sigma_A \in \mathrm{Mor}_{\mathbf{C}}(A, B)$. $F(f) \in \mathrm{Mor}_{\mathbf{C}'}(F(A), F(B))$, and $\sigma_B^{-1} G(g)\sigma_A = f = \sigma_B^{-1} GF(f)\sigma_A$, so by the injectivity of the maps shown above, we have $g = F(f)$, and so (ii) is also satisfied.

$\boxed{\Leftarrow}$ By (i) we have that every $X \in Ob(\mathbf{C}')$ is isomorphic to one of the form $F(A)$ for a certain $A \in Ob(\mathbf{C})$. Let $\theta_X : X \to F(A)$ denote this isomorphism. Suppose that we have $Y \in Ob(\mathbf{C}')$, $Y \cong F(B)$, and $g : X \to Y$. Then, define $G : \mathbf{C}' \to \mathbf{C}$ by $G(X) = A$, and $G(g) = \phi_{A,B}^{-1}(\theta_Y g \theta_X^{-1})$, where ϕ_{AB} is the bijection $\mathrm{Mor}_{\mathbf{C}}(A, B) \to \mathrm{Mor}_{\mathbf{C}'}(F(A), F(B))$ given by F.

Note that G is a functor because F is a functor, and so the maps $\phi_{A,B}$ send the identity to the identity and behave well with respect to compositions, that is $\phi_{A,C}(g \circ f) = \phi_{B,C}(g) \circ \phi_{A,B}(f)$. In particular, the maps ϕ_{AB} send isomorphisms to isomorphisms. Then we define $\forall B \in Ob(\mathbf{C})$, $\epsilon_B =$

$\phi^{-1}_{B,GF(B)}(\theta_{F(B)}) = G(\theta_Y) : B \to GF(B)$, which is an isomorphism. Given a morphism $f : A \to B$ we have $\epsilon_B^{-1} GF(f)\epsilon_A = G(\theta_Y^{-1} F(f)\theta_X)$, so applying the definition of G we have that $\epsilon_B^{-1} GF(f)\epsilon_A = \phi^{-1}_{AB}(F(f)) = f$. On the other hand, every $g : X \to Y$ is of the form $F(f)$ for a certain f, and satisfies $FG(g) = FGF(f) = F(\phi^{-1}_{AB}(\theta_Y g \theta_X^{-1})) = \theta_Y g \theta_X^{-1}$. In conclusion, we have built a functor $G : \mathbf{C}' \to \mathbf{C}$ and isomorphisms of functors $\theta = (\theta_X)_{X \in Ob(\mathbf{C}')}$, $\epsilon = (\epsilon_A)_{A \in Ob(\mathbf{C})}$ that make F into an equivalence of categories. □

Definition 1.6. We say that $Z \in Ob(\mathbf{C})$ is *terminal* if $\forall A \in Ob(\mathbf{C}) \, \exists!$ morphism $f \in \mathrm{Mor}_{\mathbf{C}}(A, Z)$. A terminal object is usually denoted by 1.

Definition 1.7. We say that $Z \in Ob(\mathbf{C})$ is *initial* if $\forall A \in Ob(\mathbf{C}) \, \exists!$ morphism $f \in \mathrm{Mor}_{\mathbf{C}}(Z, A)$. An initial object is usually denoted by 0.

Definition 1.8. Let $X, Y, S \in Ob(\mathbf{C})$, and let $f : X \to S$, $g : Y \to S$ be morphisms. The *fibred product* of X and Y over S (built with respect to f and g) is a triple $(X \times_S Y, p_1, p_2)$, with $X \times_S Y \in Ob(\mathbf{C})$, $p_1 : X \times_S Y \to X$, and $p_2 : X \times_S Y \to Y$ morphisms called *projections*, such that p_1, p_2 make commutative the diagram with f and g, and the following property is satisfied: $\forall Z \in Ob(\mathbf{C})$ and morphisms $h_1 : Z \to X$, $h_2 : Z \to Y$ making commutative the diagram with f and g, $\exists! \theta : Z \to X \times_S Y$ such that makes the following diagram commutative:

$$\begin{tikzcd}
Z \arrow[drr, bend left, "h_1"] \arrow[ddr, bend right, "h_2"'] \arrow[dr, dotted, "\theta"] & & \\
& X \times_S Y \arrow[r, "p_1"] \arrow[d, "p_2"] & X \arrow[d, "f"] \\
& Y \arrow[r, "g"] & S
\end{tikzcd}$$

If S is a terminal object in $\mathbf{C}$, the fibred product is called just *product* and it is denoted $X \times Y$. It is trivial that it satisfies the following universal property: $\forall Z \in Ob(\mathbf{C})$ and morphisms $h_1 : Z \to X$, $h_2 : Z \to Y$, $\exists! \theta : Z \to X \times Y$ such that $h_1 = p_1\theta$ and $h_2 = p_2\theta$. In this situation, we usually denote $\theta = (h_1, h_2)$.

Definition 1.9. Let $(X_i)_{i \in I}$ be a collection of objects in $\mathbf{C}$. The *sum* of the objects $(X_i)_{i \in I}$ is a pair $(\coprod_{i \in I} X_i, (q_i)_{i \in I})$, where $\coprod_{i \in I} X_i \in Ob(\mathbf{C})$ and $(q_i)_{i \in I}$ is a set of morphisms, one for each $i \in I$, $q_i : X_i \to \coprod_{i \in I} X_i$ that satisfy the following property: $\forall Y \in Ob(\mathbf{C})$, and $(f_i)_{i \in I}$ collection of morphisms $f_i : X_i \to Y$, $\exists! f : \coprod_{i \in I} X_i \to Y$ such that $\forall i \in I$ makes commutative the diagram

$$\begin{tikzcd}
X_i \arrow[r, "q_i"] \arrow[d, "f_i"] & \coprod_{i \in I} X_i \arrow[dl, dotted, "f"] \\
Y &
\end{tikzcd}$$

We say that the sum is *finite* if $\# I < \infty$.

Definition 1.10. Let $X \in Ob(\mathbf{C})$ and $G \subset \mathrm{Aut}_{\mathbf{C}}(X)$ a finite subgroup. The *quotient of X by G* is a pair $(X/G, p)$, where $X/G \in Ob(\mathbf{C})$ and $p : X \to X/G$ is a morphism satisfying $p = p\sigma \; \forall \sigma \in G$, such that $\forall Y \in Ob(\mathbf{C})$ and $f : X \to Y$ satisfying $f = f\sigma \; \forall \sigma \in G$, $\exists! f' : X/G \to Y$ making the following diagram commutative

$$\begin{tikzcd}
X \arrow[r, "p"] \arrow[d, "f"] & X/G \arrow[dl, dotted, "f'"] \\
Y &
\end{tikzcd}$$

Definition 1.11. Let $X, Y \in Ob(\mathbf{C})$ and $f, g : X \to Y$. We say that the pair (E, θ), with $E \in Ob(\mathbf{C})$ and $\theta : E \to X$ is an *equalizer of f and g* if $\forall Z \in Ob(\mathbf{C})$ and $h : Z \to X$ satisfying $fh = gh$, $\exists! h' : Z \to E$ such that the following diagram commutes:

$$\begin{tikzcd}
Z \arrow[r, "h"] \arrow[dr, dotted, "h'"] & X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \\
& E \arrow[u, "\theta"] &
\end{tikzcd}$$

Remark 1.2. The objects just defined may not exist in certain categories. However, it can be seen that all of them are unique up to isomorphism if they exist. See Appendix A.1 for the proofs of these uniquenesses.

Proposition 1.2. Let $\mathbf{C}$ be a category such that a terminal object exists in $\mathbf{C}$, and the fibred product of any two objects over a third one exists in $\mathbf{C}$. Then any pair of morphisms $f, g : X \to Y$ in $\mathbf{C}$ has an equalizer.

Proof. Let $f, g : X \to Y$ and $h : Z \to X$ satisfying $fh = gh$, and let $((X \times_Y X), (p_1, p_2))$ be the fibred product with respect to f, g. Now consider the maps $a = (\mathrm{id}, \mathrm{id}) : X \to X \times X$ and $b = (p_1, p_2) : X \times_Y X \to X \times X$. Let's build the fibred product of X and $X \times_Y X$ over $X \times X$ with respect to the maps a, b: $(X \times_{X \times X} (X \times_Y X), (q_1, q_2))$. Then, given $h : Z \to X$ satisfying $fh = gh$, $\exists! \theta$ which makes the following diagram commutative:

$$\begin{tikzcd}
Z \arrow[drr, bend left, "h"] \arrow[dr, dotted, "\theta"] \arrow[ddr, bend right, "h"'] & & \\
& X \times_Y X \arrow[r, "p_1"] \arrow[d, "p_2"] & X \arrow[d, "f"] \\
& X \arrow[r, "g"] & Y
\end{tikzcd}$$

As we have $(p_1\theta, p_2\theta) = (h, h)$, $\exists! \chi$ making commutative the following diagram:

$$\begin{tikzcd}
Z \arrow[drr, bend left, "h"] \arrow[dr, dotted, "\chi"] \arrow[ddr, bend right, "\theta"'] & & \\
& X \times_{X \times X} (X \times_Y X) \arrow[r, "q_1"] \arrow[d, "q_2"] & X \arrow[d, "a"] \\
& X \times_Y X \arrow[r, "b"] & X \times X
\end{tikzcd}$$

Reciprocally, any such θ in the second diagram must satisfy $p_1\theta = p_2\theta = h$ and so arises from the first diagram. Then, the pair $(X \times_{X \times X} (X \times_Y X), q_1)$ satisfies that for every $Z \in Ob(\mathbf{C})$ and any morphism $h : Z \to X$ satisfying $fh = gh$, $\exists! \chi : Z \to X \times_{X \times X} (X \times_Y X)$ satisfying $q_1\chi = h$, so it is an equalizer of f, g. □

Definition 1.12. Let $A, B \in Ob(\mathbf{C})$, and $f : X \to Y$ a morphism. We say that f is an *epimorphism* if $\forall Z \in Ob(\mathbf{C})$ and morphisms $h_1, h_2 : Y \to Z$ satisfying $h_1 f = h_2 f$ we have $h_1 = h_2$. Similarly, we say that f is a *monomorphism* if $\forall g_1, g_2 : Z \to X$ satisfying $fg_1 = fg_2$ we have $g_1 = g_2$.

Definition 1.13. Given $X, Y \in Ob(\mathbf{C})$, and $q_1 : X \to Y$, we say that q_1 *is an isomorphism of X with a direct summand of Y* if $\exists Z \in Ob(\mathbf{C})$ and $q_2 : Z \to Y$ such that $Y = X \amalg Z$, with morphisms q_1, q_2.

1.2 Profinite groups

Definition 1.14. Let I be a partially ordered set. We say that I is *directed* if for any pair $i, j \in I$, $\exists k \in I$ such that $k \geq i, k \geq j$.

Definition 1.15. A subset of a partially ordered set is called *cofinal* if $\forall i \in I$ $\exists j \in J$ such that $j \geq i$.

Definition 1.16. A *projective system* is a triple $(I, (S_i)_{i\in I}, (f_{ij})_{i\geq j})$, where I is a directed partially ordered set, $(S_i)_{i\in I}$ a collection of sets (one for each $i \in I$), and for each $i, j \in I$, $i \geq j$, $f_{ij} : S_i \to S_j$ is a map satisfying

1. $f_{ii} = \mathrm{id}_{S_i}$ for every $i \in I$
2. $f_{ik} = f_{jk} \circ f_{ij}$ for every $i, j, k \in I$ with $i \geq j \geq k$

Definition 1.17. Given a projective system $(I, (S_i)_{i\in I}, (f_{ij})_{i\geq j})$, the *projective limit* of the system, denoted $\varprojlim_{i\in I} S_i$ is the set

$$\varprojlim_{i\in I} S_i = \left\{ (x_i)_{i\in I} \in \prod_{i\in I} S_i \text{ such that } f_{ij}(x_i) = x_j \ \forall i \geq j \right\}$$

Observation 1.1. If S_i are groups and f_{ij} are group homomorphisms, then $\varprojlim S_i$ has a natural group structure. If S_i are topological spaces, $\varprojlim S_i$ can be made into a topological space by giving the product topology to $\prod_{i\in I} S_i$ and $\varprojlim S_i$ the induced topology.

Proposition 1.3. Let $(I, (S_i)_{i\in I}, (f_{ij})_{i\geq j})$ be a projective system, with $(S_i)_{i\in I}$ non-empty compact Hausdorff spaces, and f_{ij} continuous maps. Then $\varprojlim S_i$ is non-empty, compact and Hausdorff.

Proof. By the Thikonov theorem, the product of compact spaces is compact, so $\prod_{i\in I} S_i$ is compact.

If f_{ij} are continuous, and S_j is Hausdorff, then $S_j \setminus \{x_j\}$ is open in S_j, and $f_{ij}^{-1}(S_j \setminus \{x_j\})$ is open, which implies that $C'_{ij} := \{(x_i, x_j) \in S_i \times S_j$ such that $f_{ij}(x_i) = x_j\}$ is closed. Then, as the projection $\prod_{i\in I} S_i \to S_i \times S_j$ is continuous, the preimage of the set C'_{ij} (denoted C_{ij}) is closed in $\prod_{i\in I} S_i$. By definition $\varprojlim_{i\in I} S_i = \bigcap_{i\geq j} C_{ij}$ and so the projective limit is closed in $\prod_{i\in I} S_i$, and therefore compact.

Moreover, if $\varprojlim_{i\in I} S_i = \varnothing$, the complements of C_{ij} (let's denote them U_{ij}), form an open cover of $\prod_{i\in I} S_i$. By compactness, we can extract a finite subcover $\{U_{i_1,j_1}, \dots, U_{i_n,j_n}\}$. But as the set is directed, take $l \geq i_k \forall k = 1, \dots, n$, take $x \in S_l$ and let $x_{i_k} = f_{li_k}(x_l)$ and $x_{j_k} = f_{lj_k}(x_{i_k})$, and x_t arbitrary for all other index. Then, this element belongs to $\prod_{i\in I} S_i$ but is not in any of the sets $U_{i_kj_k}$, which is a contradiction that implies $\varprojlim_{i\in I} S_i \neq \varnothing$.

Finally, the product of Hausdorff spaces is Hausdorff, and any subspace of a Hausdorff space with the induced topology is also Hausdorff. □

Definition 1.18. A *profinite group* π is a group that is isomorphic to the projective limit of a system of finite groups $\{\pi_i\}$. If we turn every π_i into a topological space by giving it the discrete topology, π has also a structure of topological space. An *homomorphism of profinite groups* is just a homomorphism of topological groups.

Observation 1.2. Using Proposition 1.3, and the fact that the discrete topology in a finite set is a compact Hausdorff topology, it is clear that every profinite group is a compact Hausdorff space. Therefore, every continuous and bijective group morphism between profinite groups is also a homeomorphism, and therefore an isomorphism of profinite groups.

Example 1.1.

- Every finite group can be seen to be isomorphic to the projective limit of the system $\{G/H\}_H$, where H are the normal subgroups of G, ordered by $G/H \geq G/H' \iff H' \supseteq H$ and with projection transition maps. Therefore every finite group is profinite.
- Consider p a prime number, I the set of positive integers ordered in the usual way. The groups $(\mathbb{Z}/p^n\mathbb{Z})_{n>0}$, with usual projection transition maps, form a projective system whose limit is the set of p-adic integers $\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$.

Proposition 1.4. If $(\pi_j)_{j\in J}$ are profinite groups, then $\prod_{j\in J}\pi_J$ is a profinite group.

Proof. Let $\pi_j = \varprojlim_{i\in I_j}\pi_i$, with transition maps f^j_{nm}. Consider κ the set of sets of the form $K = \{i_{j_1}, \dots, i_{j_n}\}$ where each $j_m \in J$ and $i_{j_m} \in I_{j_m}$. Consider also the system of finite groups $\tau_K = (\prod_{i\in K}\pi_i)_{K\in\kappa}$. Let's define an order in κ by $K \geq K' \iff \forall i \in K'$, and $i \in I_j, \exists l \in I_j \cap K$ such that $l \geq i$ in I_j. If $K \geq K'$, let's define the morphism of groups $f_{KK'}$ as the product of the transition maps f^j_{li}.

Then $\varprojlim_{K\in\kappa}\tau_K$ is a profinite group. Note that an element of $\varprojlim_{K\in\kappa}\tau_K$ is totally determined by the coordinates $K = \{i\}$ where i ranges over all possible indexes in $\coprod I_j$. Then, we can define a natural group homomorphism from $\varprojlim_{K\in\kappa}\tau_K \to \prod_{j\in J}\prod_{i\in I_j}\pi_i$ by the identity on each respective index i. That map has image $\prod_{j\in J}\pi_j$ and is injective. Therefore, $\varprojlim_{K\in\kappa}\tau_K \cong \prod_{j\in J}\pi_j$, which concludes the proof. □

Proposition 1.5 (Subgroups of profinite groups)**.** Let $\pi = \varprojlim_{i\in I}\pi_i$ be a profinite group, and $\pi' \subset \pi$ a subgroup of π. Then

i) π' is open $\iff$ π' is closed and of finite index.

ii) π' is closed $\Rightarrow$ π' is profinite

Proof. i) As π is a topological group, fixed an $a \in \pi$, the map $m_a : \pi \to \pi$ defined by $\sigma \mapsto a\sigma$ is continuous. Then, if π' is open, all the cosets $g\pi'$ are open. Therefore, $\pi' = \pi \setminus \bigcup_{g\notin\pi'} g\pi'$, and so π' is closed. Moreover, as π is compact, we can extract a finite cover from the open cover $\bigcup_{g\in\pi} g\pi'$, and so π' has finite index. Reciprocally, if π' is closed and of finite index, we have $\pi' = \pi \setminus \bigcup_{i=1}^{n} g_i\pi'$, and so π' is open.

ii) Let $\pi' = \pi \setminus (\pi \cap \bigcup_{\alpha\in\Gamma} V_\alpha)$, where $V_\alpha = (\prod_{i\in J_\alpha} U_i \times \prod_{i\notin J_\alpha}\pi_i)$ for certain J_α finite subsets of I. Now fix an α and let $V = V_\alpha$. Using that the set I is directed, we can take $l \geq j$, $\forall j \in J_\alpha$, and let $U_l = \{x \in \pi_l$ such that $f_{li}(x_l) \in U_i, \forall i \in J_\alpha\}$.

Then $\pi \cap V = \pi \cap (\prod_{i\neq l}\pi_i \times U_l)$. Now denote by l_α the corresponding index for each set V_α. Then, $\pi' = \pi \cap \prod_{i\in I} C_i$, where $C_{l_\alpha} = \pi_{l_\alpha} \setminus U_{l_\alpha}$ and $C_i = \pi_i$ if $i \neq l_\alpha$ for any $\alpha \in \Gamma$. Now take $\rho_i = \{x \in C_i$ such that $\exists z \in \pi'$ with $z_i = x\}$. We have $\pi' = \pi \cap \prod_{i\in I}\rho_i$, where each ρ_i is a subgroup of π_i. Then, we have $\pi' \cong \varprojlim_{i\in I}\rho_i$, where the morphisms are the restrictions of f_{ij} to ρ_i. □

We also state two more properties of profinite groups (without proof) that we will need at a certain point.

Proposition 1.6 ([7], Proposition 1.1.10)**.** Let $(I, (\pi_i)_{i\in I}, (f_{ij})_{i\geq j})$ be a projective system of finite groups, with f_{ij} surjective morphisms. Let π be the projective limit of the system. Then, the projection morphisms $f_i : \pi \to \pi_i$ are surjective.

Proposition 1.7 ([2], Corollary 1)**.** i) In a compact, totally disconnected group, every neighbourhood of 1 contains an open normal subgroup.

ii) If G is a profinite group, $G \cong \varprojlim G/H$, where H runs through all open normal subgroups of G.

1.2.1 π-sets

Definition 1.19. Let π be a profinite group. A π-set is a set E equipped with an action $\pi \times E \to E$, that is continuous if we give E the discrete topology. A morphism of π-sets is a map $f : E \to E'$ satisfying $f(\sigma e) = \sigma f(e)$, $\forall \sigma \in \pi, e \in E$.

It is immediate from these definitions that π-sets form a category. The finite sets with a continuous action of π also form a category, that we will denote π-**sets**. We are mainly interested in finite π-sets, so unless otherwise stated, when we refer to a π-set we are assuming that it is finite.

Observation 1.3. We should also note that a bijective morphism of π sets is an isomorphism: Indeed, let $f : E \to E'$ be a bijective morphism of π-sets, and let $e' = f(e)$. Then, $f^{-1}(\sigma e') = f^{-1}(\sigma f(e)) = f^{-1}(f(\sigma e)) = \sigma e = \sigma f^{-1}(e')$.

Proposition 1.8. Let π be a profinite group (not necessarily finite) acting on a set E. Then,

i) The action is continuous $\iff$ $\forall e \in E$ the stabilizer $\pi_e = \{\sigma \in \pi : \sigma e = e\}$ is open in π.

ii) If E is finite, the action is continuous $\iff$ the kernel of the action, $\{\sigma \in \pi : \sigma e = e \; \forall e \in E\}$ is open in π.

iii) Any finite transitive π-set is isomorphic to π/π' for a certain π' open subgroup of π.

Proof. i) Let $A : \pi \times E \to E$ denote the action. Let $e \in E$. If the action is continuous, the set $U = A^{-1}(\{e\}) = \{(\sigma, g) \text{ such that } \sigma g = e\}$ is open. Then, $U \cap (\pi \times \{e\}) = \pi_e$ is also open. Reciprocally, let πe denote the orbit of $e \in E$. Let $e' \in \pi e$, and $\tau_{e'} \in \pi$ such that $\tau_{e'} e = e'$. Then, $m^{-1}_{\tau_{e'}}(\pi_e) = \{\sigma : \sigma e' = e\}$ is open. Then, $A^{-1}(\{e\}) = \bigcup_{e' \in \pi e}(m^{-1}_{\tau_{e'}}(\pi_e) \times \{e'\})$ is open, and so the action is continuous.

ii) The kernel of the action (denoted π') is the intersection of all the stabilizers. If E is finite, then if the stabilizers are open the kernel is also open. Reciprocally, using Proposition 1.5, we know that π' has finite index. Let $(\tau_i)_{i=1}^n$ be the representatives of the different classes, and suppose that for $i = 1, \dots, m$, with $m \leq n$, we have $\tau_i e = e \Rightarrow \tau_i \pi' e = e$. Then $\pi_e = \bigcup_{i=1}^m \tau_i \pi'$, and so the stabilizers are open.

iii) Let $e \in E$ and let $\pi' = \pi_e$. Then, consider the morphism of π-sets $f : \pi/\pi' \to E$ given by $f(\pi') = e$, and $f(\sigma\pi') = \sigma e$. It is a well defined morphism of π-sets and it is surjective, because E is transitive. It is also injective: Indeed, let τ, σ such that $f(\tau\pi') = f(\sigma\pi') \Rightarrow \sigma e = \tau e \Rightarrow \tau^{-1}\sigma e = e \Rightarrow \tau^{-1}\sigma \in \pi'$, and so they're representatives of the same class $\Rightarrow f$ is injective. In conclusion, f is an isomorphism of π-sets.

□

2. Galois Categories

Definition 2.1. Let $\mathbf{C}$ be a category and $F : \mathbf{C} \to \mathbf{sets}$ a functor from $\mathbf{C}$ to the category of finite sets. We say that the pair $(\mathbf{C}, F)$ is a *Galois category*, or that $\mathbf{C}$ is a Galois category with *fundamental functor* F, if the following axioms 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 An initial object exists in $\mathbf{C}$, finite sums exist in $\mathbf{C}$, and for any object in $\mathbf{C}$ the quotient by a finite group of automorphisms exists.

G3 Any morphism u in $\mathbf{C}$ factors as $u = u'u''$, where u' is a monomorphism and u'' is an epimorphism. Every monomorphism $f : X \to Y$ in $\mathbf{C}$ is an isomorphism of X with a direct summand of Y.

G4 The functor F transforms terminal objects into terminal objects and commutes with fibred products.

G5 The functor F transforms initial objects into initial objects, commutes with finite sums, sends epimorphisms to epimorphisms and commutes with passage to the quotient by a finite group of automorphisms

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

2.1 Examples of Galois Categories

Example 2.1. The pair $(\mathbf{sets}, \mathrm{id})$, where **sets** is the category of finite sets and id the identity functor, is a Galois Category.

Proof. It is immediate that the identity functor satisfies $G4 - G6$, so we just have to check that the axioms $G1 - G3$ are satisfied in **sets**.

G1 One-element sets are terminal objects in **sets**.

Given X, Y, S finite sets, and morphisms $f : X \to S$, $g : Y \to S$, the set $Z = \{(x, y) \in X \times Y \text{ such that } f(x) = g(y)\}$, together with morphisms $p_1 : Z \to X$, $(x, y) \mapsto x$ and $p_2 : Z \to Y$, $(x, y) \mapsto y$ is a fibred product of X and Y over S. Indeed, the projection morphisms form a commutative diagram with f, g, as every pair $(x, y) \in Z$ satisfies that $f(x) = g(y)$. Moreover, given any finite set T and morphisms $h_1 : T \to X$, $h_2 : T \to Y$ satisfying $fh_1 = gh_2$, there is a map $\theta : T \to Z$ given by $t \mapsto (h_1(t), h_2(t))$, which satisfies $p_i\theta = h_i$. It is the unique map with that property: Indeed, if we had another map $T \to Z$ with this property, and given $t \in T$ we denote its image in Z by (x, y), $p_i\theta = h_i \Rightarrow x = h_1(t), y = h_2(t)$. In conclusion this proves that the fibred product of any 2 objects over a third one exists in $\mathbf{C}$.

G2 **sets** has an initial object, which is the empty set $\varnothing$: Given any finite set X, there is a unique map (the void map) from $\varnothing$ to X.

Given a finite collection of sets $(X_i)_{i=1}^n$, we can take the disjoint union of the sets $X = \coprod_{i=1}^n X_i$, and together with the inclusion maps $q_i : X_i \to X$, we will check that this is the sum of the $(X_i)_{i=1}^n$. Indeed, given an object Z, and maps $f_i : X_i \to Z$, there is a unique map $f : X \to Z$ satisfying $f_i = fq_i$, which is given by $f(x) = f_i(x)$ if $x \in X_i$. This proves that **sets** has finite sums.

Given a finite set X and a subgroup of automorphisms $G \subseteq \mathrm{Aut}(X)$, consider the set X/G to be the set of orbits of X under G, that is, the set of elements of X with the equivalence relation that $x \sim y \iff \exists \sigma \in G$ such that $\sigma(x) = y$. Let's denote by p the projection map that sends every element to its class. It is clear that $p = p\sigma \; \forall \sigma \in G$. A morphism $f : X \to Y$ such that $f = f\sigma$

satisfies that every element in an orbit has the same image by f, so this defines a map $g : X/G \to Y$ given by $g(\overline{x}) = f(x)$, and this map is clearly unique. This proves that the quotient of X by any finite group of automorphisms exists in **sets**.

G3 First we will prove that in **sets** a map is an epimorphism if and only if it is surjective, and that it is a monomorphism if and only if it is injective. Let $f : X \to Y$ be a surjective map between finite sets, and $g, h : Y \to Z$ satisfying $hf = gf$. Let $y \in Y$. Then $y = f(z)$ for a certain z and so we have $hf(z) = gf(z) \Rightarrow h(y) = g(y)$. This proves that $h = g$ and so f is an epimorphism. Reciprocally, suppose that we have an epimorphism $f : X \to Y$. Then consider the maps $h, g : Y \to \{0, 1\}$ such that $g(y) = 1\ \forall y \in Y$ and $h(y) = 1$ if $y \in f(X)$ and $h(y) = 0$ if $y \notin f(X)$. We do have $gf = hf$, so as f is an epimorphism we have that $g = h$, which allows us to conclude that $f(X) = Y$, i.e. f is surjective. Now let $f : X \to Y$ be an injective map, and let $g, h : Z \to X$ satisfying $fh = fg$. If there exists a $z \in Z$, such that $h(z) \neq g(z)$ that means that $fg(z) \neq fh(z)$ by injectivity, which is a contradiction. In conclusion we have $g = h$ and f is a monomorphism. Reciprocally, suppose that $f : X \to Y$ is a monomorphism. If it is not injective, $\exists x, y \in X$ such that $f(x) = f(y)$. Then, let $g : X \to X$ be the identity, and $h : X \to X$ given by $h(x) = y, h(y) = x$, and $h(x') = x' \forall x' \neq x, y$. Clearly $fg = fh$ but $g \neq h$, which is a contradiction that proves that f is injective.

Now it is clear that every morphism factors as the composition of an epimorphism and a monomorphism, as every morphism of sets is a surjection followed by an injection: $X \to f(X) \to Y$. Moreover, given a monomorphism $f : X \to Y$ (that is, an injective map), we have that $Y = f(X) \amalg (Y \setminus f(X))$, so every monomorphism $X \to Y$ is an isomorphism of X with a direct summand of Y.

□

Example 2.2. The category π-**sets** of finite sets endowed with a continuous action of a profinite group π, is a Galois category with fundamental functor $F : \pi$-**sets** $\to$ **sets** being the forgetful functor.

Proof. G1 Terminal object: One-element sets endowed with the trivial action of π are terminal objects in π-**sets**.

Fibred product: Given E_1, E_2, S π-sets, and morphisms $f_1 : E_1 \to S$, $f_2 : E_2 \to S$, the set $Z = \{(x, y) \in E_1 \times E_2$ such that $f_1(x) = f_2(y)\}$, with the induced action $\sigma(x, y) = (\sigma x, \sigma y)$, together with morphisms $p_1 : Z \to E_i$, $(x, y) \mapsto x$ and $p_2 : Z \to E_2$, $(x, y) \mapsto y$, is a fibred product of E_1 and E_2 over S. To prove this claim, we first need to check that both Z and the projection maps are well defined. Z is clearly a finite set and, if $f(x) = f(y)$, then $\sigma f_1(x) = \sigma f_2(y)$ and so $f_1(\sigma x) = f_2(\sigma y)$, which proves that $\forall \sigma \in \pi$, and $(x, y) \in Z$, $\sigma(x, y) \in Z$ and so Z is a well defined π-set. Moreover, $p_1(\sigma(x, y)) = p_1(\sigma x, \sigma y) = \sigma x = \sigma p_1(x, y)$. The same calculation works for p_2 and so the projections are indeed morphisms of π-sets.

It is clear that the projections form a commutative diagram with f_1, f_2, as every pair $(x, y) \in Z$ satisfies that $f_1(x) = f_2(y)$. Moreover, given any π-set E' and morphisms $h_1 : E' \to E_1$, $h_2 : E' \to E_2$ satisfying $f_1 h_1 = f_2 h_2$, there is a morphism $\theta : E' \to Z$ given by $e' \mapsto (h_1(e'), h_2(e'))$. This is clearly a morphism of π-**sets** as $\theta(\sigma e') = (h_1(\sigma e'), h_2(\sigma e')) = \sigma(h_1(e'), h_2(e')) = \sigma\theta(e')$. θ satisfies $h_i = p_i\theta$ and it is the unique map with that property, as given an element $e' \in E'$, any other map $\phi : E' \to Z$ with that property maps e' to a certain element (x, y) and $p_i\phi = h_i \Rightarrow x = h_1(e'), y = h_2(e')$ $\forall e' \in E$, so $\phi = \theta$. This proves that the fibred product of any 2 objects over a third one exists in π-**sets**.

G2 Initial object: π-**sets** has an initial object, which is the empty set $\varnothing$.

Finite sums: Given a finite collection of π-sets $(E_i)_{i=1}^n$, we can take the disjoint union $E = \coprod_{i=1}^n E_i$, and define a π action induced by the action on each of the sets E_i. Together with the inclusion maps $q_i : E_i \to E$ (which are clearly morphisms of π-sets by the way that we have defined the action on E) we will check that this is the sum of the $(E_i)_{i=1}^{n}$. Indeed, given an object Z, and maps $f_i : E_i \to Z$, there is a unique morphism of π-sets defined by $f : E \to Z$ satisfying $f_i = fq_i$, which is given by $f(x) = f_i(x)$ if $x \in X_i$. This proves that π-**sets** has finite sums.

Quotient by a subgroup of automorphisms: Given a π-set E and a subgroup of automorphisms $G \subseteq \mathrm{Aut}(E)$, consider the set E/G to be the set of orbits of E under G, that is, the set of elements of X with the equivalence relation that $x \sim y \iff \exists \tau \in G$ such that $\tau(x) = y$. Consider p the projection map that sends every element to its class. Let's check that the action induced by E on E/G is still well defined. Indeed, if $x \sim y$, then $\exists \tau \in G$ such that $\tau(x) = y$. Then, $\tau(\sigma x) = \sigma\tau(x) = \sigma y$, and so $\sigma x \sim \sigma y$. With that definition of action in E/G it is immediate that p is a morphism of π-sets.

It is also clear that $p = p\sigma\ \forall \sigma \in G$. Then, given a morphism $f : X \to Y$ satisfying that $f = f\sigma$, it means that every element in an orbit has the same image by f, so this defines a map $g : X/G \to Y$ given by $g(\overline{x}) = f(x)$, which is unique. Moreover $g(\sigma\overline{x}) = f(\sigma x) = \sigma f(x) = \sigma g(\overline{x})$, which proves that g is a morphism of π-**sets**. In conclusion, the quotient of X by any finite group of automorphisms exists in π-**sets**.

G3 First we will prove that in π-**sets** a map is an epimorphism if and only if it is surjective, and it is a monomorphism if and only if it is injective. The implications *injective* $\Rightarrow$ *monomorphism* and *surjective* $\Rightarrow$ *epimorphism* are clear.

Suppose that we have an epimorphism $f : X \to Y$. Then consider the maps $h, g : Y \to \{0, 1\}$ such that $g(y) = 1 \forall y \in Y$ and $h(y) = 1$ if $y \in f(X)$ and $h(y) = 0$ if $y \notin f(X)$, with trivial action of π. These are morphisms of π-**sets** (note that $y \in f(X) \iff \sigma y \in f(X) \forall \sigma \in \pi$). We do have $gf = hf$, so as f is an epimorphism we have $g = h$ and so $f(X) = Y$, and f is surjective. Now suppose that $f : X \to Y$ is a monomorphism. If it is not injective, $\exists x, y \in X, x \neq y$ such that $f(x) = f(y)$. Then consider Z the fibred product of X over Y with respect to f twice, and the projection maps p_1, p_2. It is clear that $fp_1 = fp_2$. We have that $(x, y) \in Z$ but $p_1(x, y) = x \neq y = p_2(x, y)$. So $fp_1 = fp_2$ but $p_1 \neq p_2$, which is a contradiction, and this allows us to conclude that that f must be injective.

Every morphism of sets is a surjection followed by an injection: $X \to f(X) \to Y$. Moreover, if f is a morphism of π-sets, then $f(X)$ is also a π-set, with action given by $\sigma f(x) = f(\sigma x)$. Therefore, the factorization of every morphism as an epimorphism followed by a monomorphism exists in π-**sets**. Moreover, given a monomorphism $f : X \to Y$ (that is, an injective map), we have that $Y = f(X) \amalg (Y \setminus f(X))$, so every monomorphism $X \to Y$ is an isomorphism of X with a direct summand of Y.

G4-G5 It is clear from the construction above that the forgetful functor commutes with finite sums, fibred products, and quotients by groups of automorphisms, and that sends initial objects, terminal objects, and epimorphisms to initial objects, terminal objects and epimorphisms in **sets**.

G6 A morphism in π-**sets** is an isomorphism if and only if it is bijective (Observation 1.3). Therefore, if $F(u)$ is bijective, u is also bijective and therefore it is an isomorphism.

□

The following example is more relevant, as we will see later that it is a particular case of the general situation of finite étale coverings that we want to deal with. We will first need a lemma that characterizes free separable algebras over fields.

Observation 2.1. Let $\{w_i\}_{i=1}^{n}$ be a basis of B over A. It is immediate from the definition that B is free separable over A if and only if $\det(\mathrm{Tr}(w_iw_j)_{i,j}) \in A^*$.

Lemma 2.1. Let K be a field with algebraic closure $\overline{K}$. Let B be a finite dimensional K-algebra. Then, the following assertions are equivalent:

i) B is free separable over K
ii) $B \otimes_K \overline{K}$ is free separable over $\overline{K}$.
iii) $B \otimes_K \overline{K} \cong \overline{K}^n$ as $\overline{K}$-algebras, for some $n \geq 0$
iv) $B \cong \prod_{i=1}^t B_i$ as K-algebras, where each B_i is a separable field extension of K.

Proof. $\boxed{(i) \iff (ii)}$ Let $\{w_1, \dots, w_n\}$ be a base of B over K. Then, $\{w_1 \otimes 1, \dots, w_n \otimes 1\}$ is a $\overline{K}$ base of $B \otimes_K \overline{K}$. As $(w_i \otimes 1)(w_j \otimes 1)(w_k \otimes 1) = w_iw_jw_k \otimes 1$, $\mathrm{Tr}_{B/K}(w_iw_j) = \mathrm{Tr}_{B/K}((w_i \otimes 1)(w_j \otimes 1))$, and so B is free separable over K if and only if $B \otimes \overline{K}$ is free separable over $\overline{K}$.

$\boxed{(ii) \Rightarrow (iii)}$ Using the structure theorem of Artin rings ([1], Theorem 8.7), every finite algebra over a field must be of the form $B \otimes \overline{K} = \prod_{i=1}^n C_i$, with C_i certain local $\overline{K}$-algebras with nilpotent maximal ideals $\mathfrak{m}_i$. As $B \otimes_K \overline{K}$ is free separable over $\overline{K}$, then each C_j must be free separable: Indeed, if $\{w_j^i\}_j$ is a basis of C_i, then $\{e_{i,j} = (0, \dots, 0, w_j^i, 0, \dots, 0)\}_{i,j}$ is a basis of $B \otimes_K \overline{K}$. Then the determinant of the matrix $\mathrm{Tr}(e_{i,j}e_{i',j'})$ is the product of the determinants of the matrices $\{\mathrm{Tr}(w_{j_1}^i w_{j_2}^i)\}_{j_1,j_2}$, and so $B \otimes_K \overline{K}$ is free separable if and only if each C_i is free separable. Now fix a certain index i and a linear map $\phi : C_i \to \overline{K}$. Then, $\exists c \in C_i$ such that $\phi(x) = Tr(cx)$, $\forall x \in C_i$. If we pick $x \in \mathfrak{m}_i$, then the map $y \mapsto (cx)y$ is nilpotent, because x is nilpotent. Using the Jordan form of the linear map, it is easily seen that a nilpotent map has all eigenvalues equal to 0, and therefore it has trace 0. This implies that $\mathfrak{m}_i \subseteq \ker \phi$. As that works for every ϕ, then we must have $\mathfrak{m}_i = \{0\}$, and so C_j is a field. Since it is a finite extension of $\overline{K}$, it must be $\overline{K}$ itself.

$\boxed{(iii) \Rightarrow (ii)}$ Take the basis $e_i = (0, \dots, 0, 1, 0, \dots, 0)$. Then, $\mathrm{Tr}(e_ie_j) = \mathrm{id}$, so $B \otimes_K \overline{K}$ is free separable.

$\boxed{(iv) \Rightarrow (iii)}$ By the primitive element theorem, we have $B_i = K(\beta_i) \cong K[X]/(f_i)$, where f_i is the irreducible polynomial of β_i over K, and it is a separable polynomial as B_i is free separable. Then, $\overline{B_i} := B_i \otimes_K \overline{K} \cong \overline{K}[X]/(f_i)$. f_i splits into different linear factors in $\overline{K}[X]$, as $\overline{K}$ is algebraically closed, so $f_i = \prod_{i=1}^{\deg(f_i)}(X - \alpha_{ij})$. Then by the Chinese reminder theorem, $\overline{B_i} \cong \prod_{i=1}^{\deg(f_i)} \overline{K}[X]/(X - \alpha_{ij}) \cong \overline{K}^{\deg(f_i)}$. In conclusion, $B \otimes \overline{K} \cong \overline{K}^n$, where $n = \sum_{i=1}^t \deg(f_i)$.

$\boxed{(iii) \Rightarrow (iv)}$ Using again the structure theorem for Artinian rings ([1], Theorem 8.7), let's write $B = \prod_{i=1}^t B_i$, with B_i local K-algebras with nilpotent maximals $\mathfrak{m}_i$. For each $b \in B$, the sub-algebra $K[b]$ is isomorphic to $K[X]/(f_b)$, for some f_b. Tensoring the injective map $K[X]/(f_b) \to K[b] \to B$ with $\overline{K}$ we get an injective map $\overline{K}[X]/(f_b) \to B \otimes_K \overline{K}$, as K is a field and therefore an absolutely flat ring. As $B \otimes_K \overline{K}$ has no nilpotent elements other than 0, $\overline{K}[X]/(f_b)$ has no nilpotent elements other than 0. In particular: (a) if b is nilpotent, then $X^n \in (f_b)$ for a certain n, and as (f_b) is prime we have $X \in (f_b) \Rightarrow b = 0$. This proves that $\mathfrak{m}_i = \{0\}$ and so all B_i are fields. (b) the polynomial (f_b) is separable. If $b = (b_1, \dots, b_t) \in B$, then f_b is the least common multiple of the irreducible polynomials of b_i, so all of them are separable. This proves that B_i is a separable field extension of K. □

Example 2.3. Let K be a field and $\mathfrak{Sch}(K)$ denote the category of schemes over K. Let $\mathbf{C}$ be the category whose objects are affine schemes over K of the form $\mathrm{Spec}(B)$, where B is a free separable K-algebra, and whose morphisms are morphisms of affine schemes. Let $F : \mathbf{C} \to$ **sets** be the functor $\mathrm{Mor}_{\mathfrak{Sch}(K)}(\mathrm{Spec}(K_s), -)$. Then $(\mathbf{C}, F)$ is a Galois Category.

Proof. Using [3] Proposition II.2.3, we know that given K-algebras A, B, there is a bijective correspondence between morphisms of K-algebras $A \to B$ and morphisms of affine schemes over K, $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$. We will use this result several times in the verification of the axioms G1-G6. Let's also note that a free separable K-algebra A can be written as $A = \prod_{i=1}^{n} K_i$, where each K_i is a separable field extension of K. Then, the prime ideals of A are of the form $\mathfrak{p}_i = (K_1, \times \cdots \times K_{i-1} \times \{0\} \times K_{i+1} \times \cdots \times K_n)$, and so $\mathrm{Spec}(A)$ is a topological space of n points $\{P_i\}$, each one corresponding to the ideal $\mathfrak{p}_i$. The topology on $\mathrm{Spec}(A)$ is the discrete topology and the sheaf of rings is given by $\mathcal{O}(P_i) = K_i$. A morphism $\mathrm{Spec}(K_s) \to \mathrm{Spec}(A)$ is then totally characterized by the image of the unique point in $\mathrm{Spec}(K_s)$, that must be one of the points $P_i \in \mathrm{Spec}(A)$, and an embedding $K_i \to K_s$.

G1 Terminal object: $\mathrm{Spec}(K)$ is a terminal object in the category of schemes over K, and as K is a free separable K-algebra, $\mathrm{Spec}(K)$ is also terminal in $\mathbf{C}$.

Fibred product: $(\mathrm{Spec}(B \otimes_A C), (p_1, p_2))$ is a fibred product of $\mathrm{Spec}(B)$ and $\mathrm{Spec}(C)$ over $\mathrm{Spec}(A)$, where $p_1 : \mathrm{Spec}(B \otimes_A C) \to \mathrm{Spec}(B)$ is the morphism of schemes over K corresponding to the morphism of K-algebras $B \to B \otimes_A C$, $b \mapsto b \otimes 1$; and $p_2 : \mathrm{Spec}(B \otimes_A C) \to \mathrm{Spec}(C)$ corresponding to $C \to B \otimes_A C$, $c \mapsto 1 \otimes c$ ([3], Chapter II, Theorem 3.3).

To prove that the fibred product of any two objects over a third one exists in $\mathbf{C}$, it is enough to show that $B \otimes_A C$ is a free separable K-algebra if A, B, C are free separable K-algebras. If B, C are free separable, then $B \otimes_K \overline{K} \cong \overline{K}^n$, $C \otimes_K \overline{K} \cong \overline{K}^m$ as $\overline{K}$-algebras. We have $(B \otimes_K C) \otimes_K \overline{K} \cong (B \otimes_K \overline{K}) \otimes_K (C \otimes_K \overline{K}) \cong \overline{K}^{nm}$. On the other hand we have $(B \otimes_A C) \otimes_K \overline{K} \cong (B \otimes_K \overline{K}) \otimes_A (C \otimes_K \overline{K})$. Then we have the surjective map $(B \otimes_K \overline{K}) \otimes_K (C \otimes_K \overline{K}) \to (B \otimes_K \overline{K}) \otimes_A (C \otimes_K \overline{K})$ mapping $b \otimes_K c \mapsto b \otimes_A c$. The kernel of this map must be an ideal of $(B \otimes_K \overline{K}) \otimes_K (C \otimes_K \overline{K}) \cong \overline{K}^{nm}$, so it is isomorphic to $\overline{K}^{l}$, for a certain $l \leq nm$. Then $(B \otimes_K \overline{K}) \otimes_A (C \otimes_K \overline{K}) \cong \overline{K}^{nm-l}$, and so $B \otimes_A C$ is a free separable K-algebra.

G2 Initial object: $\mathrm{Spec}(0)$ is an initial object in $\mathbf{C}$.

Finite sums: Let $(\mathrm{Spec}(A_i))_{i=1}^{n} \in Ob(\mathbf{C})$. Let $(\prod_{i=1}^{n} A_i, (p_i)_{i=1}^{n})$ be the product of the algebras A_i. It is immediate from Lemma 2.1 (iv) that $\prod_{i=1}^{n} A_i$ is a free separable K-algebra. Let $f_i : \mathrm{Spec}(A_i) \to \mathrm{Spec}(B)$ be morphisms in $\mathbf{C}$, and $\phi_i : B \to A_i$ be the corresponding morphisms of K-algebras. Then $\exists! \phi : B \to \prod_{i=1}^{n} A_i$ satisfying that $p_i \phi = \phi_i$. Let $f : \mathrm{Spec}(\prod_{i=1}^{n} A_i) \to \mathrm{Spec}(B)$ be the morphism of affine schemes corresponding to ϕ, and $q_i : \mathrm{Spec}(A_i) \to \mathrm{Spec}(\prod_{i=1}^{n} A_i)$ be the morphisms of affine schemes corresponding to p_i. Then $f q_i = f_i \, \forall i$, and so $(\mathrm{Spec}(\prod_{i=1}^{n} A_i), (q_i)_{i=1}^{n})$ is the finite sum of $(\mathrm{Spec}(A_i))_{i=1}^{n}$. This proves that finite sums exist in $\mathbf{C}$.

Quotient by a subgroup of automorphisms: Let A be a free separable K-algebra and let G be a subgroup of automorphisms of $\mathrm{Spec}(A)$. G corresponds to a group of K-algebra automorphisms of A (that we will also denote G making an abuse of notation). Write $A = \prod_{i=1}^{n} A_i$ for certain A_i finite separable field extensions of K. For every $\sigma \in G$, the map $A_i \xrightarrow[q_i]{} A \xrightarrow[\sigma]{} A \xrightarrow[p_i]{} A_i$, where q_i is the inclusion and p_i the projection, is an automorphism of A_i. Then any K-automorphism of A is the product of K-automorphisms of the fields A_i, and so $G = \prod_{i=1}^{n} G_i$, where each G_i is a subgroup of K-automorphisms of A_i. Then, $A^G = \prod_{i=1}^{n} A_i^{G_i}$. As $A_i^{G_i}$ is a finite separable extension of K, therefore A^G is a free separable K-algebra.

Consider the inclusion morphism $p' : A^G \to A$, and its corresponding morphism of schemes $p : \mathrm{Spec}(A) \to \mathrm{Spec}(A^G)$. Suppose that we have a morphism $f : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ satisfying that $f = f\sigma \; \forall \sigma \in G$, and let f' be the corresponding morphism of rings $f' : B \to A$. We have then $\sigma' f' = f' \; \forall \sigma' \in G' \Rightarrow f'(B) \subseteq A^G$, and so we can restrict the co-domain to A^G: $g' : B \to A^G$.

Clearly $p'g' = f'$, and g' is unique with this property. So the pair $(\text{Spec}(A^G), p)$ is the quotient of A by G in $\mathbf{C}$.

G3 We will prove first that every epimorphism of K-algebras is surjective. Let $f : X \to Y$ be an epimorphism and suppose that it is not surjective. Write $Y = \prod_{i=1}^n B_i$, with B_i is a separable field extension of K. Now consider $\pi_i(f(A))$ the projection on the $i-th$ coordinate. If $\pi_i(f(A)) \neq 0$ then $K \subseteq \pi_i(f(A)) \subseteq B_i$, and as B_i is integral over K, it is also integral over $\pi_i(f(A))$, and therefore $\pi_i(f(A))$ is a field ([1], Proposition 5.17), and we can write $f(A) = \prod_{i=1}^n K_i$, where each K_i is either 0 or a separable field extension of K contained in B_i. If f is not surjective, then $\exists j$ such that $K_j \neq B_j$. Suppose that $j = 1$ without loss of generality. Now let $G_i = \text{Gal}(K_s/K_i)$, where K_s is a separable closure of K, and let also $B_1 = K(\alpha)$. As $K_1 \neq B_1$, $\exists \tau \in \text{Gal}(K_s/K_1)$ such that $\tau(\alpha) \neq \alpha$. Then consider the automorphism $B \to B$ given by $\sigma = (\tau, \sigma_2, \dots, \sigma_n)$, where each $\sigma_i \in G_i$. Clearly $\sigma f = \text{id} f$ but $\sigma \neq \text{id}$, which is a contradiction. This proves that every epimorphism is surjective, and we have also obtained that if $f : A \to B$ is a morphism between 2 free separable K-algebras, then $f(A)$ is a free separable K-algebra.

Factorization of morphisms: Every morphism of K-algebras $u : A \to B$ factors as an epimorphism followed by a monomorphism: $A \mapsto f(A) \mapsto B$. By the bijective correspondence between morphisms of K-algebras and morphisms of schemes over K, monomorphisms correspond to epimorphisms and epimorphisms to monomorphisms. Then, every map $\text{Spec}(B) \to \text{Spec}(A)$ factors as an epimorphism followed by a monomorphism, $\text{Spec}(B) \to \text{Spec}(f(A)) \to \text{Spec}(A)$.

Monomorphisms are direct summands: Let $f : \text{Spec}(A) \to \text{Spec}(B)$ be a monomorphism in $\mathbf{C}$, corresponding to the surjective map $\varphi : B \to A$. φ induces an isomorphism $B/\ker(\varphi) \cong A$. Write $B = \prod_{i=1}^n B_i$, where each B_i is a separable field extension of K. As $\ker(\varphi)$ is an ideal of B, it is of the form $\prod_{i=1}^n K_i$, where each K_i is either 0 or B_i. Let $\{i_1, \dots, i_t\}$ be the indices such that $K_i = B_i$. Let $\psi : B \to \prod_{j=1}^t K_{i_j} =: C$ be the projection on these coordinates. It is now clear that $B \cong A \times \prod_{j=1}^t K_{i_j}$, so then $\text{Spec}(B) = \text{Spec}(A) \amalg \text{Spec}(C)$ and so f is an isomorphism of $\text{Spec}(A)$ with a direct summand of $\text{Spec}(B)$.

G4 Terminal objects: $\#\text{Mor}_{\mathfrak{Sch}(K)}(\text{Spec}(K_s), \text{Spec}(K)) = 1$, so F maps terminal objects in $\mathbf{C}$ to terminal objects in **sets**.

Fibred products: There is a bijective correspondence between $\text{Mor}_{\mathfrak{Sch}(K)}(\text{Spec}(K_s), \text{Spec}(B \otimes_A C))$ and pairs of morphisms $\text{Spec}(K_s) \to \text{Spec}(B)$, $\text{Spec}(K_s) \to \text{Spec}(C)$ that agree when composed with the maps $f : \text{Spec}(B) \to \text{Spec}(A)$ and $g : \text{Spec}(C) \to \text{Spec}(A)$. Then, $F(\text{Spec}(B \otimes_A C))$ is the set $\{(h_1, h_2) \in F(\text{Spec}(B)) \times F(\text{Spec}(C))$ such that $F(f)(h_1) = F(g)(h_2)\}$, which is a fibred product of $F(\text{Spec}(B))$ and $F(\text{Spec}(C))$ over $F(\text{Spec}(A))$ in **sets**.

G5 Initial object: $\text{Mor}_{\mathfrak{Sch}(K)}(\text{Spec}(K_s), \text{Spec}(0)) = \varnothing$, so F sends initial objects to initial objects.

Sums: Suppose that $A = \coprod_{i=1}^n A_i$, with A_i a free separable K-algebra. By the remark made at the beginning of the proof, it is clear that $\text{Mor}_{\mathfrak{Sch}(K)}(\text{Spec}(K_s), \text{Spec}(A)) \cong \coprod_{i=1}^n \text{Mor}_{\mathfrak{Sch}(K)}(\text{Spec}(K_s), \text{Spec}(A_i))$. Then, $F(\coprod_{i=1}^n \text{Spec}(A_i))$ is the disjoint union $\coprod_{i=1}^n F(\text{Spec}(A_i))$, and so F commutes with finite sums.

Epimorphisms: Let $A = \coprod_{i=1}^n A_i$ and $B = \prod_{i=1}^m B_i$ the usual expressions as products of separable extensions of K. An epimorphism $f : \text{Spec}(A) \to \text{Spec}(B)$ corresponds to a monomorphism $\phi : B \to A$. We will now prove that it has to be an injective map. Indeed, suppose that $\exists x, y \in A$ such that $f(x) = f(y)$. Then take $\text{id} = \psi_1 : A \to A$ and $\psi_2 : A \to A$ defined by $a \mapsto a + x - y$. $\psi_1 \neq \psi_2$ but $\phi\psi_1 = \phi\psi_2$, which is a contradiction. Now we want to check that $F(f)$ is an epimorphism. It will be enough to show that $\forall g \in F(\text{Spec}(B)) = \text{Mor}_{\mathfrak{Sch}(K)}(\text{Spec}(K_s), \text{Spec}(B))$, $g = f \circ h$, for a certain $h \in F(A)$. Let $g = (g, g^{\#}) \in F(B)$. Then, $(g, g^{\#})$ is defined by $g(\mathrm{Spec}(K_s)) = P_i$ and the embedding $B_i \hookrightarrow K_s$. As ϕ is injective, the image of f is dense in $\mathrm{Spec}(B)$ (Proposition A.1). The topology on $\mathrm{Spec}(B)$ is the discrete topology and therefore f is surjective. Then, $\exists Q_j \in \mathrm{Spec}(A)$ such that $f(Q_j) = P_i$. Consider B_i as a subfield of A_j through the map on stalks $B_i \hookrightarrow A_j$ given by $f^{\#}$. A_j is an algebraic extension of B_i and so we can extend the morphism $B_i \hookrightarrow K_s$ to a morphism $\tau : A_j \hookrightarrow K_s$. Now consider $(h, h^{\#}) \in F(A)$ defined by $h(\mathrm{Spec}(K_s)) = Q_j$ and the embedding τ, and we have $(g, g^{\#}) = (f, f^{\#}) \circ (h, h^{\#})$.

Passage to the quotient: Let $A = \prod_{i=1}^{n} A_i$ and $A^G = \prod_{i=1}^{n} A_i^{G_i}$, where $K \subseteq A_i^{G_i} \subseteq A_i$. Let $\{P_i\}_{i=1}^{n}$ and $\{P_i'\}_{i=1}^{n}$ be the points on the underlying topological space of $\mathrm{Spec}(A)$ and $\mathrm{Spec}(A^G)$, respectively. Note that every morphism of schemes over K, $\mathrm{Spec}(K_s) \to \mathrm{Spec}(A^G)$, defined by a point P_i' and an embedding $\tau' : A_i^{G_i} \hookrightarrow K_s$ gives rise to a morphism of schemes $\mathrm{Spec}(K_s) \to \mathrm{Spec}(A)$ defined by the point P_i and extending the immersion τ' to $\tau : A_i \hookrightarrow K_s$. Note that $A_i \subseteq A_i^{G_i}$ is a Galois extension, and therefore there are as many possible extensions of τ' to A_i as $[A_i : A_i^{G_i}]$, each one given by the composition of τ' by an element of G_i.

Reciprocally, every morphism of schemes over K $\mathrm{Spec}(K_s) \to \mathrm{Spec}(A)$, defined by a point P_i and an embedding $\tau : A_i \hookrightarrow K_s$ gives rise to a morphism of schemes $\mathrm{Spec}(K_s) \to \mathrm{Spec}(A^G)$ defined by the point P_i' and composing τ with the inclusion $A_i^{G_i} \hookrightarrow A_i$. Two morphisms $f, g : \mathrm{Spec}(K_s) \to \mathrm{Spec}(A)$ with the same image give the same morphism $\mathrm{Spec}(K_s) \to \mathrm{Spec}(A^G)$ if and only if the image of the topological space $\mathrm{Spec}(K_s)$ is the same and the respective embeddings are the same on $A_i^{G_i}$, that is, if $f = g\sigma$ for a certain $\sigma \in G$. In conclusion, $F(A^G)$ is the set of orbits of $F(A)$ under $F(G)$, and so F commutes with passage to the quotient.

G6 This is a direct consequence of the Yonneda Lemma. See [4], Corollary 1.4.7.

□

2.2 Statement of the main theorem

Proposition 2.1. Let $(\mathbf{C}, F)$ be a small Galois category, Then, $\mathrm{Aut}(F)$ is a profinite group acting continuously on $F(X)$, $\forall X \in Ob(\mathbf{C})$.

Proof. The group of automorphisms of a finite set is its group of permutations. The automorphism group $\mathrm{Aut}(F)$ is a subgroup of $\prod_{X \in Ob(\mathbf{C})} S_{F(X)}$[2], where $S_{F(X)}$ is the permutation group of $F(X)$. In particular, $\mathrm{Aut}(F) = \{(\sigma_X)_X \in \prod_{X \in Ob(\mathbf{C})} S_{F(X)}$ such that $\forall Z, Y \in Ob(\mathbf{C})$ and $f : Y \to Z, \sigma_Z F(f) = F(f)\sigma_Y\}$. Now fix $Z, Y \in Ob(\mathbf{C})$ and $f : Y \to Z$. The set $C_f = \{(\sigma_X)_X \in \prod_{X \in Ob(\mathbf{C})} S_{F(X)}$ such that $\sigma_Z F(f) = F(f)\sigma_Y\}$ is closed, as it is the finite union of the closed sets $(\prod_{X \in Ob(\mathbf{C}), X \neq Z, Y} S_{F(X)}) \times \{\sigma_Y\} \times \{\sigma_Z\}$, where (σ_Y, σ_Z) is a pair satisfying $\sigma_Z F(f) = F(f)\sigma_Y$. Then $\mathrm{Aut}(F)$ is the intersection of closed sets C_f as f varies among all morphisms in $\mathbf{C}$, and therefore it is a closed subgroup of $\prod_{X \in Ob(\mathbf{C})} S_{F(X)}$.

Each $S_{F(X)}$ is finite and in particular profinite, and so $\prod_{X \in Ob(\mathbf{C})} S_{F(X)}$ is the product of profinite groups and it is profinite (Proposition 1.4). Then $\mathrm{Aut}(F)$ is a closed subgroup of a profinite group, so it is also profinite by Proposition 1.5.

The map $\mathrm{Aut}(F) \times F(X) \to F(X)$ defined by $((\sigma_X)_{X \in Ob(\mathbf{C})}, a) = \sigma_X(a)$ defines an action of $\mathrm{Aut}(F)$ on $F(X)$ with open kernel $\mathrm{Aut}(F) \cap (\prod_{Ob(\mathbf{C}) \ni Y \neq X} S_{F(Y)} \times \{\mathrm{id}_X\})$, so it is a continuous action by Proposition 1.8. □

[2] The product must range over a set. Therefore, when we write $\prod_{X \in Ob(\mathbf{C})} S_{F(X)}$, we are implicitely requiring $\mathbf{C}$ to be a small category.

Remark 2.1. Given any morphism $f : Y \to Z$, and $(\sigma_X) \in \mathrm{Aut}(F)$, the map $F(f) : F(Y) \to F(Z)$ respects the $\mathrm{Aut}(F)$ action, because it is satisfied that $\sigma_Z F(f) = F(f)\sigma_Y$. Therefore, given $(\mathbf{C}, F)$ a Galois category, we can define a functor $H : \mathbf{C} \to \mathrm{Aut}(F)$-**sets** by mapping every $X \in \mathbf{C}$ to the set $F(X)$ endowed with the $\mathrm{Aut}(F)$ action just defined, and every $f : Y \to Z$ to $F(f)$, which we have just seen that is indeed a morphism of $\mathrm{Aut}(F)$-**sets**.

Remark 2.2. As already remarked, the argument we made in order to regard $\mathrm{Aut}(F)$ as a profinite group only holds if $\mathbf{C}$ is a small category. In the following argumentation, we can replace any category by an equivalent one, so it will be enough to require our categories to be *essentially small*, that is, equivalent to a small category.

Theorem 2.1 (Main Theorem)**.** *Let* $(\mathbf{C}, F)$ *be an essentially small Galois category. Then*

i) The functor $H : \mathbf{C} \to \mathrm{Aut}(F)$-**sets** *is an equivalence of categories.*

ii) If π *is a profinite group such that the categories* $\mathbf{C}$ *and* π-**sets** *are equivalent by an equivalence that, when composed with the forgetful functor* π-**sets** $\to$ **sets** *yields the functor* F*, then* π *is canonically isomorphic to* $\mathrm{Aut}(F)$.

iii) If F' *is a second fundamental functor on* $\mathbf{C}$*, then* F *and* F' *are isomorphic.*

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

Note that the axioms of a Galois category, together with the main theorem, give an axiomatic characterization of all the categories that are equivalent to π-**sets**, for a certain profinite group π. The purpose of the rest of the chapter is to develop the necessary tools to prove the theorem. The strategy of the proof is a little bit intricate: We will first build a profinite group π, define an action of π on $F(X)$ and prove that this induces an equivalence H' between $\mathbf{C}$ and π-**sets**, that yields F when composed with the forgetful functor. Then we prove (ii) and apply it to the equivalence already constructed to prove (i).

From now on, let $(\mathbf{C}, F)$ be a small Galois category.

2.3 Subobjects and connected objects

Definition 2.2. Let $X \in Ob(\mathbf{C})$. Consider the set $\{Y \to X \text{ monomorphism }\}/\sim$, Where $\sim$ is the equivalence relation that identifies two monomorphisms $f : Y \to X \sim f' : Y' \to X \iff \exists Y \xrightarrow{\cong} Y'$ isomorphism making the diagram commutative:

$$\begin{tikzcd} Y \arrow[r, "\cong"] \arrow[d, "f"'] & Y' \arrow[dl, "f'"] \\ X & \end{tikzcd}$$

Every equivalence class is called a *subobject* of X.

Lemma 2.2. f is a monomorphism $\iff$ F(f) is injective.

Proof. Let $f : Y \to X$. First we prove that f is a monomorphism $\iff$ $p_1 : Y \times_X Y \to Y$ is an isomorphism. If f is a monomorphism, then $(Y, \mathrm{id}_Y, \mathrm{id}_Y)$ satisfies the definition of fibred product. Therefore we have $Y \times_X Y \cong Y$ and $p_1 = \mathrm{id}_Y\theta$, where θ is the isomorphism $Y \times_X Y \to Y \Rightarrow p_1$ is an isomorphism. Reciprocally, consider the following commutative diagram:

$$\begin{tikzcd}
Y \arrow[rrd, bend left, "\mathrm{id}"] \arrow[rd, dotted, "\theta"] \arrow[rdd, bend right, "\mathrm{id}"'] & & \\
& Y \times_X Y \arrow[r, "p_1"] \arrow[d, "p_2"] & Y \arrow[d, "f"] \\
& Y \arrow[r, "f"] & X
\end{tikzcd}$$

We have $p_1\theta = \mathrm{id}$, but as p_1 is an isomorphism, $\Rightarrow \theta = p_1^{-1}$. Now, as $p_2\theta = \mathrm{id} \Rightarrow p_1 = p_2$.

Then, given $Z \in Ob(\mathbf{C})$, and $h_1, h_2 : Z \to Y$ satisfying $fh_1 = fh_2$, $\exists\phi$ making commutative the diagram with the fibred product, and so we have $h_1 = p_1\phi$, $h_2 = p_2\phi$, but as $p_1 = p_2 \Rightarrow h_1 = h_2$. Then f is a monomorphism.

Now using the fact that F commutes with fibred products, that every monomorphism in **sets** is injective and $G6$, we have the following implications: $F(f)$ injective $\iff$ $F(p_1)$ isomorphism $\iff$ p_1 isomorphism $\iff$ f monomorphism. □

Lemma 2.3. Two monomorphisms $f : Y \to X$ and $f' : Y' \to X$ are representatives of the same subobject of $X \iff F(f)(F(Y)) = F(f')(F(Y'))$ as subsets of $F(X)$.

Proof. $\boxed{\Rightarrow}$ Let $f = f'\theta$, with θ an isomorphism. Then, $F(f)(F(Y)) = F(f')F(\theta)(F(Y))$ but $F(\theta)$ is an isomorphism and therefore surjective, and so $F(\theta)(F(Y)) = F(Y') \Rightarrow F(f)(F(Y)) = F(f')F(Y')$.

$\boxed{\Leftarrow}$ As F commutes with fibred products, we have the following commutative diagrams:

$$\begin{tikzcd}
Y \times_X Y' \arrow[r, "p_1"] \arrow[d, "p_2"] & Y \arrow[d, "f"] & F(Y \times_X Y') \arrow[r, "F(p_1)"] \arrow[d, "F(p_2)"] & F(Y) \arrow[d, "F(f)"] \\
Y' \arrow[r, "f'"] & X & Y' \arrow[r, "F(f')"] & F(X)
\end{tikzcd}$$

But $F(Y \times_X Y') \cong \{(y, y') \in F(Y) \times F(Y') | F(f)(y) = F(f')(y')\}$. As $F(f)$, $F(f')$ are injective, and the images of $F(Y)$, $F(Y')$ are the same in $F(X)$, then $F(p_1)$ and $F(p_2)$ are bijective, and so they're isomorphisms. Using $G6$, we have that p_1, p_2 are isomorphisms. Now using the commutative diagram of the fibred product, we have $f'p_2p_1^{-1} = f$, and so f, f' are representatives of the same subobject of X. □

To simplify notation, if $Y \to X$ is a monomorphism, we will usually identify $F(Y)$ with its image in $F(X)$ and write $F(Y) \subset F(X)$.

Definition 2.3. We say that an object $X \in Ob(\mathbf{C})$ is *connected* if it has exactly 2 subobjects, $0 \to X$ and $\mathrm{id} : X \to X$.

Proposition 2.2. Every object in $\mathbf{C} \neq 0$ is the sum of its connected subobjects.

Proof. Let's argue by induction on $\#F(X)$. If $\#F(X) = 1$, then X is connected, because there are only two possible subsets of $F(X)$, the empty set and $F(X)$ itself. Now suppose that $\#F(X) \geq 1$ and that X is not connected. Then, $\exists q_1 : Y \to X$ subobject of X which is not the initial subobject nor the total (in particular, $\varnothing \neq F(Y) \subsetneq F(X)$). As q_1 is a monomorphism, applying G3 we know that $\exists q_2 : Z \to X$ such that $X \cong Y \amalg Z$. Note that $F(q_2)$ is injective and so q_2 is a monomorphism, and therefore representative of a subobject of X. We have $\#F(Y), \#F(Z) < \#F(X)$, and so applying the induction hypothesis on Y, Z, we have that $Y = \coprod_{i=1}^{n} Y_i$ and $Z = \coprod_{j=1}^{m} Z_j$, where Y_i is a connected subobject of Y and Z_j is a connected subobject of Z. As the composition of monomorphisms is also a monomorphism, then Y_i, Z_j are also connected subobjects of X. Therefore $X = (\coprod_{i=1}^{n} Y_i) \amalg (\coprod_{j=1}^{m} Z_j)$, and so X is the sum of connected subobjects of X. Now we should check that every connected subobject is in that sum. Consider $X \cong \coprod_{i=1}^{n} X_i$ and Y_1 a subobject of X. We can make the same construction and obtain $X \cong \coprod_j Y_j$. Let $\coprod_i X_i \cong \coprod_j Y_j$, with X_i, Y_j connected, and consider the monomorphism $q_i : X_i \to \coprod_i X_i$. Composing with the isomorphism $\theta : \coprod_i X_i \to \coprod_j Y_j$, we obtain a monomorphism $X_i \to \coprod_j Y_j$. By connectedness of X_i and Y_j, we must have $F(X_i) = F(Y_j)$ for a certain j, and so they're the same subobject. □

Let's see some examples of connected objects and how this last proposition applies in several Galois categories.

Example 2.4. An object in the category of π-**sets** is connected if and only if it is transitive. Indeed, if E is not transitive, then we can split it into orbits: $E = \coprod_{i=1}^{n} E_i$, and the inclusion map $f_i : E_i \to E$ is a monomorphism of π-**sets**, which is not the identity nor the empty map. Then, E is not connected. Reciprocally, let $f : E' \to E$ an injective morphism of π-**sets**, with E transitive. If $\text{im}(f) = \varnothing$, then f is a representative of the initial subobject. Otherwise, let $e \in \text{im}(f)$, $e = f(d)$. $\forall e' \in E$, $\exists \sigma$ such that $\sigma f(d) = \sigma e = e'$. Then, $e' = f(\sigma d)$ and so f is surjective. In conclusion, f is a representative of the identity subobject. This proves that E is connected.

Moreover, every $X \in Ob(\pi\text{-}\mathbf{sets})$ is the sum of its orbits, which are the connected subobjects of E. This is an example of the statement of the proposition above.

Example 2.5. Let $\mathbf{C}$ be the category of affine schemes of the form $\text{Spec}(B)$, with B a free separable K-algebra (see Example 2.3). An object in $\mathbf{C}$ is connected if and only if $X = \text{Spec}(A)$, with A a separable field extension of K. Indeed, a monomorphism $\text{Spec}(B) \to \text{Spec}(A)$ corresponds to an epimorphism $A \to B$. Then $\text{Spec}(A)$ is connected if and only if the only epimorphisms $A \to A'$ are either isomorphisms or the zero map. If A is a field, this is clearly satisfied, as every ring morphism $A \to A'$ is either 0 or injective. Reciprocally, if A is not a field, it can be written as $A = \prod_{i=1}^{m} A_i$, where each A_i is a separable field extension of K. Then each projection $A \to A_i$ is a surjective morphism of K-algebras and therefore it is a subobject of A different from $0, A$.

Then, last proposition states that in $\mathbf{C}$, the decomposition $\text{Spec}(A) = \coprod_{i=1}^{n} \text{Spec}(A_i)$ is the expression of A as the sum of its connected subobjects.

Proposition 2.3. Let A be a connected object in $\mathbf{C}$, and $a \in F(A)$. Then, $\forall X \in Ob(\mathbf{C})$ the map

$$\begin{aligned} \text{Mor}_{\mathbf{C}}(A, X) &\longrightarrow F(X) \\ f &\longmapsto F(f)(a) \end{aligned}$$

is injective.

Proof. Let $f, g \in \text{Mor}_{\mathbf{C}}(A, X)$. Let (C, θ) be the equalizer of f, g, which we know that exists by Proposition 1.2. As F commutes with fibred products, it also commutes with equalizers and so we have that $(F(C), F(\theta))$ is an equalizer of $F(f)$, $F(g)$, and so $F(C) \cong \{b \in F(A) : F(f)(b) = F(g)(b)\}$. Therefore $F(\theta) : F(C) \to F(A)$ is injective, and θ is a monomorphism. Moreover, $F(C) \neq \varnothing$, because $a \in F(C)$, and by the connectedness of A we must have $F(C) = F(A)$, so $F(\theta)$ is an isomorphism. By G6, θ is an isomorphism, which implies $f = g$. □

Remember that our purpose is to define an action on $F(X)$ by a profinite group π. To do that, we will replace the functor F by an isomorphic functor that will provide us with a more natural way to define an action.

Now let's consider the set $I = \{(A,a)|A \text{ connected }, a \in F(A)\}/\sim$, with $\sim$ the equivalence relation $(A,a) \sim (B,b) \iff \exists f : A \to B$ isomorphism such that $F(f)(a) = b$. Let's define a partial order on I by $(A,a) \geq (B,b) \iff \exists f : A \to B$ such that $F(f)(a) = b$. It is straightforward to check that this is indeed an order relation on I, and that I is directed:

- Reflexivity: Taking $f = \mathrm{id}_A$, we have $F(\mathrm{id})(a) = a$, so $(A,a) \geq (A,a)$.
- Anti-symmetry: If $(A,a) \geq (B,b)$, and $(B,b) \geq (A,a)$, there exist $f : A \to B$ and $g : B \to A$ such that $F(f)(a) = b$ and $F(g)(b) = a$. But then we have $F(fg)(b) = b$ and $F(gf)(a) = a$, so by the injectivity of the last proposition, $fg = \mathrm{id}_B$, $gf = \mathrm{id}_A$, and so f is an isomorphism and therefore (A,a) and (B,b) are representatives of the same class in I.
- Transitivity: Let $(A,a) \geq (B,b) \geq (C,c) \in I$ and $f : A \to B$, $g : B \to C$ the maps satisfying $F(f)(a) = b$, $F(g)(b) = c$. Then, $g \circ f : A \to B$ satisfies $F(g \circ f)(a) = F(g) \circ F(f)(a) = F(g)(b) = c$, and so $(A,a) \geq (C,c)$.
- I is directed: Let $(A,a),(B,b) \in I$ and consider the element $(C,(a,b))$, where C is the connected component of $A \times B$ containing the element (a,b). Then $(C,(a,b)) \in I$. Then, compose the monomorphism $C \to A \times B$ with the projections $p_1 : A \times B \to A$ and $p_2 : A \times B \to B$. Let's name the resulting maps f_1 and f_2. Then, $F(f_1)(a,b) = a$ and $F(f_2)(a,b) = b$, so $(C,(a,b)) \geq (A,a),(B,b)$.

We will denote $(A,a) \geq_f (B,b)$ if we want to specify the morphism $f : A \to B$ satisfying $F(f)(a) = b$.

Proposition 2.4. There is an isomorphism of functors

$$\begin{aligned} \varinjlim_{(A,a)\in I} \mathrm{Mor}_{\mathbf{C}}(A,-) &\longrightarrow \quad F(-) \\ f &\longmapsto F(f)(a) \end{aligned}$$

Proof. First let's check that the limit $\varinjlim_{(A,a)\in I} \mathrm{Mor}_{\mathbf{C}}(A,X)$ is well defined $\forall X \in Ob(\mathbf{C})$. Indeed, given $(A,a) \geq_f (B,b) \in I$, we have morphisms $f_{BA} : \mathrm{Mor}_{\mathbf{C}}(B,X) \to \mathrm{Mor}_{\mathbf{C}}(A,X)$ defined by $g \mapsto g \circ f$. These morphisms form an injective system, as $f_{AA} = \mathrm{id}_A$ and if $(A,a) \geq_f (B,b) \geq_g (C,c)$ we have $f_{CA}(h) = h \circ (g \circ f) = (f_{BA} \circ f_{CB})(h)$.

Then, let's consider the maps $\phi_A : \mathrm{Mor}_{\mathbf{C}}(A,X) \to F(X)$ given by $f \mapsto F(f)(a)$. If $(A,a) \geq_g (B,b) \in I$, then $\phi_A \circ f_{BA} = \phi_B$, because $\phi_A(f_{BA}(f)) = F(f \circ g)(a) = F(f)(b) = \phi_B(f)$. Therefore, by the properties of the injective limit, $\exists!$ map $\phi : \varinjlim_{(A,a)\in I} \mathrm{Mor}_{\mathbf{C}}(A,X) \to F(X)$ given by $\phi(f) = \phi_A(f)$ if $f \in \mathrm{Mor}_{\mathbf{C}}(A,X)$. Now let's prove that it is an isomorphism, i.e. a bijective map.

Suppose that we have $F(f)(a) = F(g)(b)$ for certain $(A,a),(B,b) \in I$. Let C be the connected component of $A \times B$ such that $c = (a,b) \in F(C)$, and let p_1', p_2' denote the compositions of the projection maps $p_1 : A \times B \to A$ and $p_2 : A \times B \to B$ with the monomorphism $C \to A \times B$. Then we have $f_{AC}(f) = fp_1'$, $f_{BC}(g) = gp_2'$, so $F(fp_1')(c) = F(gp_2')(c) \Rightarrow f_{AC}(f) = f_{BC}(g)$, and this implies that $\overline{f} = \overline{g}$ in $\varinjlim_{(A,a)\in I} \mathrm{Mor}_{\mathbf{C}}(A,X)$. To prove surjectivity, take $x \in F(X)$ and consider $f : A \to X$ the connected component of X such that $x \in F(A)$. Then $(A,x) \in I$ and $F(f)(x) = x$.

Finally, we have to check that the map induces an isomorphism of functors. Let $X, Y \in Ob(\mathbf{C})$. Then, the following diagram

$$\begin{tikzcd}
\varinjlim_{(A,a)\in I} \mathrm{Mor}_{\mathbf{C}}(A, X) \arrow[r] \arrow[d, "f\circ -"] & F(X) \arrow[d, "F(f)\circ -"] \\
\varinjlim_{(A,a)\in I} \mathrm{Mor}_{\mathbf{C}}(A, Y) \arrow[r] & F(Y)
\end{tikzcd}$$

is commutative, as an element $g \in \varinjlim_{(A,a)\in I} \mathrm{Mor}_{\mathbf{C}}(A, X)$ is sent to $F(f \circ g)(a) = F(f) \circ F(g)(a)$. This completes the proof and we have an isomorphism of functors $\varinjlim_{(A,a)\in I} \mathrm{Mor}_{\mathbf{C}}(A, -) \cong F(-)$. □

2.4 Galois objects

If A is a connected object, we have the following inequalities: $\#\mathrm{Aut}_{\mathbf{C}}(A) \leq \#\mathrm{Mor}_{\mathbf{C}}(A) \leq \#F(A)$. In particular, the set of automorphisms of A is finite, and therefore it makes sense to talk about the quotient of an object by its group of automorphisms.

Definition 2.4. $A \in Ob(\mathbf{C})$ is a *Galois object* if the quotient $A/\mathrm{Aut}_{\mathbf{C}}(A)$ is a terminal object.

Observation 2.2. If $\mathbf{C}$ is a connected Galois object, using that F commutes with quotients and terminal objects, we have $F(A)/\mathrm{Aut}_{\mathbf{C}}(A)$ is terminal, so $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on $F(A)$. This implies that the chain of inequalities $\#\mathrm{Aut}_{\mathbf{C}}(A) \leq \#\mathrm{Mor}_{\mathbf{C}}(A) \leq \#F(A)$ become equalities, and so $\mathrm{Mor}_{\mathbf{C}}(A) = \mathrm{Aut}_{\mathbf{C}}(A)$. Therefore, in a connected Galois object, every endomorphism is an isomorphism.

Reciprocally, if $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on $F(A)$, $F(A)/\mathrm{Aut}_{\mathbf{C}}(A)$ is terminal, and so by axiom G6 $A/\mathrm{Aut}_{\mathbf{C}}(A)$ must also be terminal, which implies that A is Galois.

Example 2.6. In the category of π-**sets**, connected Galois objects are sets of the form π/π', where π' is an open normal subgroup of π.

Proof. We already know that a connected object must be isomorphic to π/π', with π' an open subgroup of π. First note that every endomorphism $f \in \mathrm{Aut}(\pi/\pi')$ is totally determined by $f(\pi') = a\pi'$ for a certain $a \in \pi$, because then, as f is a morphism, we have $f(\tau\pi') = \tau a \pi'$. Moreover, a, a' determine the same morphism if and only if $a'a^{-1} \in \pi'$, that is, if and only if they belong to the same lateral class. Now, if f is an automorphism, it has an inverse map, g defined by $g(\pi') = b\pi'$. We must have then $fg(\pi') = ab\pi' = \pi'$, for example $b = a^{-1}$. But for the automorphism to be well defined, we must have $a\sigma a^{-1} \in \pi'$, for every $\sigma \in \pi' \Rightarrow a \in \rho$, where ρ is the normalizer of π' in π. Then, if we want $\mathrm{Aut}(\pi/\pi')$ to act transitively on π/π', we must have that π' is normal in π. □

Example 2.7. The connected Galois objects in the category $(\mathbf{C}, F)$ of Example 2.3 are sets of the form $\mathrm{Spec}(E)$, where E is a finite Galois extension of K.

Proof. We already know that connected objects correspond to $\mathrm{Spec}(E)$, with E a separable field extension of K. We know that $\mathrm{Spec}(E)$ is connected if and only if $\mathrm{Aut}_{\mathbf{C}}(\mathrm{Spec}(E))$ acts transitively on $F(\mathrm{Spec}(E))$. Remember that F is the functor $\mathrm{Mor}_{\mathfrak{Sch}(K)}(\mathrm{Spec}(K_s), -)$. In the case where E is a field, there is a bijective correspondence between morphisms of schemes over K $\mathrm{Spec}(K_s) \to \mathrm{Spec}(E)$ and morphisms of K-algebras $E \to \mathrm{Spec}(K_s)$.

Fix $f : \mathrm{Spec}(K_s) \to \mathrm{Spec}(E)$. $\mathrm{Spec}(E)$ is connected if and only if for every morphism $g : \mathrm{Spec}(K_s) \to \mathrm{Spec}(E)$, $g = f\sigma$ for a certain $\sigma \in \mathrm{Aut}_{\mathbf{C}}(\mathrm{Spec}(E))$. Passing from the language of schemes to the language of K-algebras, that means that every K-embedding $g' : E \hookrightarrow K_s$ satisfies $g'(E) = f'(E)$, that is, E is normal, and so E is a finite Galois extension of K. □

Proposition 2.5. Let $X \in Ob(\mathbf{C})$. There exists $(A, a) \in I$ with A Galois such that the map $\mathrm{Mor}(\mathbf{C})(A, X) \to F(X)$, $f \mapsto F(f)(a)$ is bijective.

Proof. Let $Y = X^{\#F(X)}$ be the product of $\#F(X)$ copies of X. As F commutes with products, we have $F(Y) = F(X)^{\#F(X)}$. Now let's index the coordinates of Y by the elements of $F(X)$, and let $a \in F(Y)$ having as x-th coordinate the element x. Then consider A the connected component of Y such that $a \in F(A)$, and $f_x : A \to Y \to X$ be the composition of the monomorphism $A \to Y$ and the projection on the x-th coordinate $p_x : Y \to X$. Then $f_x \in \mathrm{Mor}_{\mathbf{C}}(A, X)$ and $F(f_x)(a) = x$. As a has all the elements of $F(X)$ in its coordinates, then as f_x varies we obtain all the elements $x \in F(X)$, and so the map is bijective (as we already knew about the injectivity by Proposition 2.3).

Moreover, we have also obtained that the only morphisms in $\mathrm{Mor}_{\mathbf{C}}(A, X)$ are the ones of the form f_x for a certain $x \in F(X)$. Now let's check that A is Galois. Let $a' \in F(A)$, $a' \neq a$. The map $\mathrm{Mor}_{\mathbf{C}}(A, X) \to F(X)$ given by $f \mapsto F(f)(a')$ is bijective, as it is injective and we have just seen that the two sets have the same cardinality. As $\forall g \in \mathrm{Mor}_{\mathbf{C}}(A, X)$, $g = f_x$ for a certain x, this proves that a' has all the elements of $F(X)$ in its coordinates.

Now we will prove that there is an automorphism of Y that sends a to a'. Let $a = (a_x)_{x \in F(X)}$, and let $(a') = (a_{\sigma(x)})_{x \in F(X)}$, where σ is a permutation of the set $F(X)$. Note that $\mathrm{Mor}_{\mathbf{C}}(Y, Y) = \prod_{x \in F(X)} \mathrm{Mor}_{\mathbf{C}}(Y, X)$. Now consider the map $f = \prod_{x \in F(X)} p_{\sigma(x)}$. Then, $F(f)(a) = \prod_{x \in F(X)} F(p_{\sigma(x)})(a) = (a_{\sigma(x)})_{x \in F(X)} = a'$. Taking the inverse permutation to σ we see that f is an isomorphism. Then, the map $A \to Y \xrightarrow{\sigma} Y$ is a monomorphism, which induces an automorphism $A \cong_\tau A'$ from A to another connected component A' of Y. Moreover, as $a' \in F(A) \cap F(A')$, and A, A' are connected, we must have $F(A') = F(A)$ and so $A = A'$ and therefore τ is an automorphism of A which sends a to a'. In conclusion, $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on $F(A)$, and therefore A is Galois. □

Observation 2.3. Proposition 2.5 proves that the subset $J \subset I$ corresponding to connected Galois objects is a cofinal subset of I, so

$$\varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A, -) \cong \varinjlim_I \mathrm{Mor}_{\mathbf{C}}(A, -) \cong F$$

2.5 Construction of an equivalence to π-sets

Lemma 2.4. Let A be a connected Galois object, and B a connected object such that $\mathrm{Mor}_{\mathbf{C}}(A, B) \neq \varnothing$. Then, the action

$$\begin{aligned} \mathrm{Aut}_{\mathbf{C}}(A) \times \mathrm{Mor}_{\mathbf{C}}(A, B) &\longrightarrow \mathrm{Mor}_{\mathbf{C}}(A, B) \\ (\sigma, f) &\longmapsto \quad f \circ \sigma \end{aligned}$$

is transitive.

Proof. Let $f \in \mathrm{Mor}_{\mathbf{C}}(A, B)$. Then f factors as $f = gh$ with h an epimorphism and g a monomorphism. By the connectedness of B, g must be an isomorphism, so $F(f)$ is surjective. This implies that, given $f' : A \to B$, $\exists a' \in F(A)$ such that $F(f)(a') = F(f')(a)$. As A is Galois, $\exists \sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$ such that $F(\sigma)(a) = a'$. Then, $F(f\sigma)(a) = F(f')(a)$, and by injectivity of that map, $f\sigma = f'$. □

Lemma 2.5. Let $(A,a),(B,b) \in J$, $(A,a) \geq_f (B,b)$. Given $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$, $\exists!\tau \in \mathrm{Aut}_{\mathbf{C}}(B)$ such that $\tau f = f\sigma$, and the mapping $\sigma \mapsto \tau$ is a surjective group homomorphism.

Proof. Let $F(\sigma)(a) = a'$, $b' = F(f)(a')$. Then, as B is Galois, $\exists \tau \in \mathrm{Aut}_{\mathbf{C}}(B)$ such that $F(\tau)(b) = b'$. Then, $F(f\sigma)(a) = F(\tau f)(a) \Rightarrow f\sigma = \tau f$ by the injectivity in Proposition 2.3. To prove the uniqueness, suppose that we have two automorphisms τ_1, τ_2 satisfying the property. Then $F(\tau_1\tau_2^{-1})(b) = b$, and again by injectivity we have $\tau_1\tau_2^{-1} = \mathrm{id} \Rightarrow \tau_1 = \tau_2$.

It's clear that the identity maps to the identity. Given $\sigma_1 \mapsto \tau_1$ and $\sigma_2 \mapsto \tau_2$, we have $f\sigma_1\sigma_2 = \tau_1 f\sigma_2 = \tau_1\tau_2 f$, and so $\sigma_1\sigma_2 \mapsto \tau_1\tau_2$. This proves that $\sigma \mapsto \tau$ is a group morphism. Moreover, as the action of $\mathrm{Aut}_{\mathbf{C}}(A)$ on $\mathrm{Mor}_{\mathbf{C}}(A,B)$ is transitive (Lemma 2.4), given $\tau \in \mathrm{Aut}_{\mathbf{C}}(B)$, $\exists\sigma$ such that $\tau f = f\sigma$, and so the morphism is surjective. □

Definition 2.5. This lemma gives rise to a projective system, and so we have a profinite group $\pi := \varprojlim_J \mathrm{Aut}_{\mathbf{C}}(A)$.

Proposition 2.6. $\forall X \in Ob(\mathbf{C})$, the action

$$\begin{aligned}\varprojlim_J \mathrm{Aut}_{\mathbf{C}}(A) \times \varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A,X) &\longrightarrow \varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A,X)\\ ((\sigma_A)_{A\in J}, f) &\longmapsto \quad f\circ\sigma_A^{-1}\end{aligned}$$

defines a functor $H' : \mathbf{C} \to \pi$-**sets**.

Proof. First of all, we have to check that the action is well defined. Let $f_A \in \mathrm{Mor}_{\mathbf{C}}(A,X)$, $f_B \in \mathrm{Mor}_{\mathbf{C}}(B,X)$ be representatives of the same element in $\varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A,X)$. This means that $\exists(C,c) \in J$ such that $(C,c) \geq_{f_1} (A,a)$ and $(C,c) \geq_{f_2} (B,b)$, and $f_B f_2 = f_C$, $f_A f_1 = f_C$. Then, $(\sigma_C, f_C) = f_C\sigma_C^{-1} = f_B f_2 \sigma_C^{-1}$ and $(\sigma_C, f_C) = f_C\sigma_C^{-1} = f_A f_1 \sigma_C^{-1}$. But $\sigma_A^{-1} f_1 = f_1\sigma_C^{-1}$ and $\sigma_B^{-1} f_2 = f_2\sigma_C^{-1}$. Therefore, $f_C\sigma_C^{-1} = f_A\sigma_A^{-1} f_1 = f_B\sigma_B^{-1} f_2$, so $f_B\sigma_B^{-1} = f_A\sigma_A^{-1}$ in $\varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A,X)$.

Now let's check that the action is continuous. Let $f \in \mathrm{Mor}_{\mathbf{C}}(A,X)$ be a representative of an element $\overline{f} \in \varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A,X)$. Then, its preimage by the action is the set $\bigcup_{g\in \mathrm{Mor}(A,X)} U \times \{\overline{g}\}$, where $U \subset \pi = \{(\sigma_A) \in \pi : g\sigma_A^{-1} = f\}$. U is open in π and therefore the preimage of $\overline{f}$ by the action is open.

Finally, we have to check that it is indeed a functor. Given a morphism $f : X \to Y$, $H'(f)$ maps $(f_A)_{A\in J} \mapsto (f \circ f_A)_{A\in J}$. Then it is clear that H' preserves compositions and maps the identity to the identity. □

Remark 2.3. We have defined a functor $H' : \mathbf{C} \to \pi$-**sets** by endowing the functor $\varprojlim_J \mathrm{Mor}_{\mathbf{C}}(A,-)$ with a continuous π-action. By the existence of the isomorphism of functors $\varprojlim_J \mathrm{Mor}_{\mathbf{C}}(A,-) \cong F(-)$ deduced in Observation 2.3, it is immediate that we can induce a π-action on $F(X)$ for every X, and that H' induces a functor $\mathbf{C} \to \pi$-**sets** that is equal to F when composed with the forgetful functor π-**sets** $\to$ **sets**.

To show that there is an equivalence of categories $\mathbf{C} \to \pi$-**sets** that gives F when composed with the forgetful functor, it is then enough to show that H' is an equivalence of categories, which is what we will proceed to do now. First we need to prove some more properties.

Proposition 2.7. Let B be a connected object in $\mathbf{C}$. Then $B \cong A/G$, for a certain A Galois and G a subgroup of automorphisms of A.

Proof. Take A Galois as in Proposition 2.5. Then, $\mathrm{Mor}_{\mathbf{C}}(A,B) \cong F(B) \cong \varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A,B)$ and $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on $\mathrm{Mor}_{\mathbf{C}}(A,B)$ by Lemma 2.4, so $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on $H'(B)$, and therefore we have $H'(B) \cong \mathrm{Aut}_{\mathbf{C}}(A)/G$, where G is the stabilizer of a certain element $f \in H'(B)$. In particular $\#F(B) = \#Aut_{\mathbf{C}}(A)/G$. Apart from that, we also have $f\sigma = f\ \forall\sigma \in G$, and therefore we have a morphism $g : A/G \to B$ induced by f. $F(g)$ is surjective, because $F(f)$ is surjective. Moreover, $\#F(A/G) = \#F(A)/G = \#\mathrm{Aut}_{\mathbf{C}}(A)/G$, and therefore $F(g)$ is an isomorphism (surjective between sets of the same cardinal). By G6, g is also an isomorphism and so $B \cong A/G$. □

Proposition 2.8. The functor H' maps connected objects to connected objects.

Proof. For every connected object B, choose A Galois such that $\mathrm{Mor}(A, B) \cong F(B)$. Then $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on $\mathrm{Mor}_{\mathbf{C}}(A, B)$. By Proposition 1.6, then also π acts transitively on $H'(B)$, and so $H'(B)$ is a transitive π-set, that is, a connected object of the category π-**sets**. □

Lemma 2.6. Let $f : X \to Z$ be an epimorphism in a Galois Category, and $g : W \to Z$ a subobject $\neq 0, Z$. Then, $W \times_Z X \to X$ is a subobject $\neq 0, X$. In particular, if $X \to Z$ is an epimorphism and X is connected, then also Z is connected.

Proof. First let's prove that it is indeed a subobject, that is, the map $p_2 : W \times_Z X \to X$ is a monomorphism. Indeed, let $s, t : Y \to W \times_Z X$ satisfying $p_2 s = p_2 t$. Therefore, composing with f on both sides we get $fp_2 s = fp_2 t$ and so $gp_1 s = gp_1 t$. As g is a monomorphism, this implies that also $p_1 s = p_1 t$. In conclusion, both s, t fit in the commutative diagram of the fibred product:

$$\begin{tikzcd}
Y \arrow[drr, bend left, "p_1 s = p_1 t"] \arrow[dr, dotted] \arrow[ddr, bend right, "p_2 s = p_2 t"'] & & \\
& W \times_Z X \arrow[r, "p_1"] \arrow[d, "p_2"] & W \arrow[d, "g"] \\
& X \arrow[r, "f"] & Z
\end{tikzcd}$$

Therefore by uniqueness we must have $s = t$. This proves that p_2 is a monomorphism, and therefore $p_2 : W \times_Z X \to X$ is a subobject of X. Now we just have to check that it is not the identity nor the initial subobject. It is enough to check that $F(W \times_Z X) \neq 0, F(X)$. Note that $F(W \times_Z X) = F(W) \times_{F(Z)} F(X) = \{(a, b) \in F(W) \times F(X) | F(f)(b) = F(g)(a)\}$.

- If $F(W \times_Z X) = F(X)$, then as f is an epimorphism it means that $\forall z \in Z$, $\exists (a, b) \in F(W) \times F(X)$ such that $F(f)(b) = z$, $F(g)(a) = z$. Then $F(g)$ is surjective, and as by hypothesis g is a monomorphism, then $F(g)$ is an isomorphism (c.f. Lemma 2.2), and therefore also g is by G6. In conclusion, $W \to Z$ is the identity subobject.
- If $F(W \times_Z X) = 0$, then $\nexists (a, b) \in F(W) \times F(X)$ satisfying $F(g)(a) = F(f)(b)$. But as f is an epimorphism, this means $\nexists a \in F(W)$ such that $F(g)(a) = z$, for any $z \in Z$, and so $F(W) = \varnothing$ and it is the initial subobject.

□

Lemma 2.7. If $f, g : X \to Y$ are two morphisms in $\mathbf{C}$ satisfying $F(f) = F(g)$, then $f = g$.

Proof. By G4, Let $\theta : E \to X$, (E, θ) the equalizer of f and g. As F commutes with equalizers, then $(F(E), F(\theta))$ is the equalizer of $F(f)$ and $F(g)$, but as the two morphisms are equal, then $F(\theta)$ is an isomorphism and so θ is itself an isomorphism, which implies that $f = g$. □

Theorem 2.2. *The functor $H' : \mathbf{C} \to \pi$-**sets** is an equivalence of categories.*

Proof. To prove the theorem, we will show that the two conditions in Proposition 1.1 hold in this situation. To prove that every π-set is of the form $H'(X)$ for $X \in Ob(\mathbf{C})$, it is enough to prove it for a transitive π-set , as every π-set is isomorphic to the direct sum of is orbits, which are transitive, and the functor H' preserves finite sums.

Note that every transitive π-set is of the form $\mathrm{Aut}_{\mathbf{C}}(A)/G$, for some $G \subseteq \mathrm{Aut}_{\mathbf{C}}(A)$, and A connected Galois. Indeed, every transitive π-set is isomorphic to a set of the form π/π', and π' is open, so using that π' is compact, it can be expressed as $\pi \cap \left(\prod_{B \neq A} \mathrm{Aut}_{\mathbf{C}}(B) \times G_A\right)$. As the projection $\pi \to \mathrm{Aut}_{\mathbf{C}}(A)$ is surjective (Proposition 1.6), then $\pi/\pi' \cong \mathrm{Aut}_{\mathbf{C}}(A)/G_A$. This means that it's enough to show that for every π-set of the form $\mathrm{Aut}_{\mathbf{C}}(A)/G$, there is an object X in $\mathbf{C}$ such that $H'(X) \cong \mathrm{Aut}_{\mathbf{C}}(A)/G$.

Now note that the map

$$\begin{aligned} \mathrm{Aut}_{\mathbf{C}}(A) &\longrightarrow \quad H'(A) \\ f &\longmapsto F(f)(a) \end{aligned}$$

is bijective (we know that the map is injective, and as A is Galois, the sets have the same cardinality). Therefore the map

$$\begin{aligned} H'(A) &\longrightarrow \mathrm{Aut}_{\mathbf{C}}(A) \\ F(f)(a) &\longmapsto \qquad f^{-1} \end{aligned}$$

is a bijection, and $F(f\sigma^{-1}) \mapsto \sigma f^{-1}$, so the map respects the π-action, and it is therefore an isomorphism of π-**sets**. Then, $H'(A/G) \cong H'(A)/G \cong \mathrm{Aut}_{\mathbf{C}}(A)/G$, which proves the first property.

As for the second property, we already know that $\mathrm{Mor}_{\mathbf{C}}(X, Y) \to \mathrm{Mor}_{\pi-\mathbf{sets}}(H'(X), H'(Y))$ is injective, by Lemma 2.7. Therefore it will be enough to prove that the sets have the same cardinality. Let's see first that we can reduce again to the case of connected objects.

- $\forall X \in Ob(\mathbf{C})$, we can write its decomposition into connected components, $X = \coprod_{i=1}^{n} X_i$, and, by the universal property of finite sums, we have $\mathrm{Mor}_{\mathbf{C}}(X, Y) \cong \prod_{i=1}^{n} \mathrm{Mor}_{\mathbf{C}}(X_i, Y)$. As H' commutes with finite sums, we also have $\mathrm{Mor}_{\mathbf{C}}(H'(X), H'(Y)) \cong \prod_{i=1}^{n} \mathrm{Mor}_{\mathbf{C}}(H'(X_i), H'(Y))$ and we can reduce to the case where X is connected.
- Let $X \to Y$ morphism. By G3 we can factor it as $X \xrightarrow{\text{epi}} Z \xrightarrow{\text{mono}} Y$. If X is connected, Lemma 2.6 tells that Z is also connected, and therefore $Z \to Y$ is a connected component of Y. This shows that any morphism $X \to Y$ factors through connected components of Y, so $\mathrm{Mor}_{\mathbf{C}}(X, Y) \cong \coprod_{j=1}^{m} \mathrm{Mor}_{\mathbf{C}}(X, Y_j)$ (for X connected). Using that H' maps connected components to connected components, we also have $\mathrm{Mor}_{\mathbf{C}}(H'(X), H'(Y)) \cong \coprod_{j=1}^{m} \mathrm{Mor}_{\mathbf{C}}(H'(X), H'(Y_j))$ so it's enough to reduce to the case where both X, Y are connected.

Now choose $A \in Ob(\mathbf{C})$ large enough so that $X \cong A/G_1$, $Y \cong A/G_2$. This can always be done: For example, one can take A a connected component of $X^{\#F(X)} \times Y^{\#F(Y)}$ and repeat the same proof of Proposition 2.5, and then use Proposition 2.7. Then we have that $H'(X) \cong \mathrm{Aut}_{\mathbf{C}}(A)/G_1$, $H'(Y) \cong \mathrm{Aut}_{\mathbf{C}}(A)/G_2$. Consider a morphism of π-**sets**, $f : \mathrm{Aut}_{\mathbf{C}}(A)/G_1 \to \mathrm{Aut}_{\mathbf{C}}(A)/G_2$. Then, $f(\tau G_1) = \tau\sigma G_2$, for a certain σ that totally characterizes f. The morphism is well defined $\iff$ two representatives of the same class are mapped to the same element $\iff$ $\forall g \in G_1, gG_1 \mapsto \sigma G_2$ $\iff$ $\forall g \in G_1, g\sigma G_2 = \sigma G_2$ $\iff$ $\forall g \in G_1, g\sigma \in \sigma G_2$ $\iff$ $G_1\sigma \subseteq \sigma G_2$. Then,

$$\#\mathrm{Mor}_{\pi-\mathbf{sets}}(H'(X), H'(Y)) = \#\{\sigma G_2 \in \mathrm{Aut}_{\mathbf{C}}(A)/G_2 \text{ such that } G_1\sigma \subseteq \sigma G_2\}$$

On the other side, the choice of A implies that $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on both $\mathrm{Mor}_{\mathbf{C}}(A, X)$ and $\mathrm{Mor}_{\mathbf{C}}(A, Y)$. Then, consider the projection morphisms $A \xrightarrow{h_1} A/G_1$ and $A \xrightarrow{h_2} A/G_2$. Given $f : X \to Y$, $\exists \sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$ such that $h_2\sigma = fh_1$.

$$\begin{tikzcd}
A \arrow[r, "h_1"] \arrow[d, "\sigma"] & A/G_1 = X \arrow[d, "f"] \\
A \arrow[r, "h_2"] & A/G_2 = Y
\end{tikzcd}$$

This implies that, for a certain $a' \in F(A)$, with $F(h_2)(a') = F(fh_1)(a)$, and σ with $F(\sigma)(a) = a'$. Then $h_2\sigma = h_2\sigma' \iff \sigma'\sigma^{-1} \in G_2 \iff G_2\sigma = G_2\sigma'$, so f uniquely determines the coset $G_2\sigma$. Reciprocally, an element $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$ gives rise to a morphism $f : X \to Y \iff h_2\sigma$ factors through A/G_1, that is, if and only if $h_2\sigma\tau = h_2\sigma, \forall \tau \in G_1 \iff \sigma G_1 \subseteq G_2\sigma$. This proves that

$$\#\mathrm{Mor}_{\mathbf{C}}(X, Y) = \#\{G_2\sigma \in \mathrm{Aut}_{\mathbf{C}}(A)/G_2 \text{ such that } \sigma G_1 \subseteq G_2\sigma\}$$

In conclusion, $\#\mathrm{Mor}_{\mathbf{C}}(X, Y) = \#\mathrm{Mor}_{\pi-\mathbf{sets}}(H'(X), H'(Y))$, and this completes the proof.

□

2.6 Proof of the main theorem

Until now we have proven that a Galois category is equivalent to π-**sets**, for a profinite group π defined in terms of Galois objects of the category (see Definition 2.5). For now, we haven't seen yet that π is isomorphic to $\mathrm{Aut}(F)$, and that's what we will do in this section, in which we finally prove Theorem 2.1.

Lemma 2.8. Let π be a profinite group, F the forgetful functor π-**sets** $\to$ **sets**. Then, $\mathrm{Aut}(F) \cong \pi$.

Proof. We want to find an isomorphism $\pi \to \mathrm{Aut}(F)$. Note that, given $\theta \in \mathrm{Aut}(F)$, the action of θ on every π-set is determined by the action on transitive π-**sets**, and as every π-set is isomorphic to one of the form π/π', with π' open subgroup of π, the action of θ is totally determined by the action on the sets of this form.

Moreover, we know that in a compact, totally disconnected group, every neighbourhood of 1 contains an open normal subgroup (Proposition 1.7). Therefore, $\exists \pi''$ open normal subgroup of π such that $\pi' \supseteq \pi''$. Then, consider the natural morphism of π-**sets** $f : \pi/\pi'' \to \pi/\pi'$. The automorphism θ of F has to commute with f. Let $\sigma \in \pi$ such that $\theta_{\pi/\pi''}(\tau\pi'') = \tau\sigma\pi''$. Then we have $f \circ \theta_{\pi/\pi''}(\tau\pi'') = \tau\sigma\pi'$, and so $\theta_{\pi/\pi'} \circ f(\tau\pi') = \tau\sigma\pi'$. As $f(\tau\pi'') = \tau\pi'$, we have then $\sigma_{\pi/\pi'}(\tau\pi') = \tau\sigma\pi'$. In conclusion, the action of $\theta \in \mathrm{Aut}(F)$ is totally determined by the coordinates $\theta_{\pi/\pi'}$, where π' runs over open normal subgroups of π.

Let π' be an open normal subgroup of π. Note that $\mathrm{Aut}_{\pi-\mathbf{sets}}(\pi/\pi') \cong \pi/\pi'$, with the following isomorphism: $\mathrm{Aut}_{\pi-\mathbf{sets}}(\pi/\pi') \to \pi/\pi'$, $f \mapsto \tau^{-1}\pi'$ if $f(\pi') = \tau\pi'$.

Now let $f : \pi/\pi' \to \pi/\pi'$ a set theoretic map commuting with all π-set automorphisms. Then, $f(\tau\pi')\sigma = f(\tau\pi'\sigma) \iff f(\pi'\tau)\sigma = f(\pi'\tau\sigma)$. Let $f(\pi') = a\pi'$. Then, $f(\pi'\sigma) = f(\sigma\pi') = f(\pi')\sigma = a\pi'\sigma$, so f is given by left product by an element of π/π'. Therefore, we can define a map $\psi : \pi \to \mathrm{Aut}(F)$ by $\psi(\sigma)_{\pi/\pi'}(\pi') = \sigma\pi'$, for every π' open normal subgroup of π. Let's proceed to check that this is an isomorphism of profinite groups.

- **Well defined**: To see that $\psi(\sigma) \in \text{Aut}(F)$, it is enough to check that it commutes with every morphism of π-**sets**, and this can be reduced to prove that it commutes with every morphism $\pi/\pi' \to \pi/\pi''$, where π', π'' are open normal subgroups of π. Let $f : \pi/\pi' \to \pi/\pi''$ defined by $f(\pi') = a\pi''$. Let $x \in \pi', x \notin \pi''$. Then, $xa\pi'' f(x\pi') = f(\pi') = a\pi'' \Rightarrow x\pi'' a = \pi'' a$, $\forall x \in \pi'$. This implies $\pi'' \supseteq \pi'$, and it's clear that $\psi(\sigma)$ commutes with f, so ψ is well defined.

- **Injective**: We have seen that an element $\theta \in \text{Aut}(F)$ is totally characterized by the coordinates $\theta_{\pi/\pi'} \in \pi/\pi'$, and $\pi \cong \varprojlim_{\pi' \text{ open normal}} \pi/\pi'$.

- **Surjective**: The fact that every morphism $\pi/\pi' \to \pi/\pi'$ commuting with all π-**sets** automorphisms is given by left product by an element of π/π', implies that every element of $\text{Aut}(F)$ has to be defined by left product by an element of $\varprojlim \pi/\pi' = \pi$.

- **Continuity**: Let $U = \text{Aut}(F) \cap \left(\prod_{i \in J} H_{E_i} \times \prod_{i \notin J} S_{E_i}\right)$, where $|J| < \infty$, and $H_{E_i} \neq S_{E_i}$. Then, $\psi^{-1}(U)$ can be expressed as $\pi \cap V$, with $V \subset \prod_{\pi' \text{ open normal}} \pi/\pi'$, V only fixing the coordinates corresponding to sets π/π', where $\pi/\pi'_{i,j}$ is isomorphic to an orbit of a set E_i. As every set has finite orbits, and J is a finite set, the coordinates that are not free in V are a finite number, and so in conclusion the preimage of an open set by ψ is open, and so ψ is continuous.

Finally, it is obvious that the functor $H : \pi - \textbf{sets} \to \text{Aut}(F)$-**sets** is the identity when seen through the isomorphism just defined.

□

Now we can begin with the proof of Theorem 2.1.

Proof. (b) Let π be a profinite group, and $H : \mathbf{C} \to \pi$-**sets** an equivalence that composed with the forgetful functor $F_1 : \textbf{sets} \to \pi$-**sets** yields F. Then we have $\text{Aut}(F_1) \cong \pi$ by Lemma 2.8. Therefore it will be enough to check that $\text{Aut}(F) \cong \text{Aut}(F_1)$.

Note that an automorphism $\epsilon \in \text{Aut}(F_1)$ induces naturally an automorphism of F, $\psi(\epsilon) := (\epsilon_{H(X)})_{X \in Ob(\mathbf{C})}$. Indeed, we have for every $A, B \in \pi$-**sets**, and $f : A \to B$ the commutative diagram

$$\begin{tikzcd}
F_1(A) \arrow[r, "F_1(g)"] \arrow[d, "\epsilon_A"] & F_1(B) \arrow[d, "\epsilon_B"] \\
F_1(A) \arrow[r, "F_1(g)"] & F_1(B)
\end{tikzcd}$$

Given $Y, Z \in Ob(\mathbf{C})$, and $f : Y \to X$ we can take $A = H(X), B = H(Y), g = H(f)$ and substituting into the diagram above, taking into account that $F_1 \circ H = F$, it yields

$$\begin{tikzcd}
F(Y) \arrow[r, "F(f)"] \arrow[d, "\epsilon_{H(Y)}"] & F(Z) \arrow[d, "\epsilon_{H(Z)}"] \\
F(Y) \arrow[r, "F(f)"] & F(Z)
\end{tikzcd}$$

Reciprocally, let's see how every automorphism of F will induce an automorphism of F_1. As H is an equivalence, we have that $\exists G : \pi\textbf{-sets} \to \mathbf{C}$, and an isomorphism of functors $\theta : \mathrm{id} \to HG$:

$$\begin{tikzcd}
A \arrow[r, "g"] \arrow[d, "\theta_A"] & B \arrow[d, "\theta_B"] \\
HG(A) \arrow[r, "HG(g)"] & HG(B)
\end{tikzcd}$$

Then let $\sigma \in \mathrm{Aut}(F)$, and take $Y = G(A)$, $Z = G(B)$, $f = G(g)$. We have then

$$\begin{tikzcd}
F(Y) \arrow[r, "F(f)"] \arrow[d, "\sigma_Y"] & F(Z) \arrow[d, "\sigma_Z"] & F_1HG(A) \arrow[r, "F_1HG(g)"] \arrow[d, "\theta_{G(A)}"] & F_1HG(B) \arrow[d, "\theta_{G(B)}"] \\
F(Y) \arrow[r, "F(f)"] & F(Z) & F_1HG(A) \arrow[r, "F_1HG(g)"] & F_1HG(B)
\end{tikzcd}$$

Then, we can define $\phi(\sigma) := (\phi(\sigma)_A)_{A \in Ob(\pi-\textbf{sets})} = (F_1(\theta_A^{-1})\sigma_{G(A)}F_1(\theta_A))_A$. Let's prove that $\phi(\sigma)$ is an automorphism of functors: Indeed, $F_1(g) = F_1(\theta_B^{-1} \circ HG(g) \circ \theta_A)$ by the diagram of the equivalence of categories. Then

$$F_1(g) \circ \phi(\sigma)_A = F_1(\theta_B^{-1} \circ HG(g) \circ \theta_A)F_1(\theta_A^{-1})\sigma_{G(A)}F_1(\theta_A) = F_1(\theta_B^{-1}) \circ F_1(HG(g)) \circ \sigma_{G(A)} \circ F_1(\theta_A)$$

And similarly,

$$\phi(\sigma)_B F_1(g) = F_1(\theta_B^{-1}) \circ \sigma_{G(B)} \circ F_1(HG(g)) \circ F_1(\theta_A)$$

Using that σ is a morphism of functors, we have that $\sigma_{G(B)}F_1HG(g) = F_1HG(g)\sigma_{G(A)}$, and so $F_1(g) \circ \phi(\sigma)_A = \phi(\sigma)_B \circ F_1(g)$ and $\phi(\sigma)$ is a well defined automorphism of the functor F_1.

So far we have defined mappings $\psi : \mathrm{Aut}(F_1) \to \mathrm{Aut}(F)$, $\phi : \mathrm{Aut}(F) \to \mathrm{Aut}(F_1)$, and it is also clear that ψ is continuous and that ψ, ϕ respect the group operations. Therefore, it will be enough to prove that $\phi\psi = \mathrm{id}_{\mathrm{Aut}(F_1)}$ and $\psi\phi = \mathrm{id}_{\mathrm{Aut}(F)}$ to see that we have an isomorphism of profinite groups $\mathrm{Aut}(F_1) \cong \mathrm{Aut}(F)$.

Let $\sigma \in \mathrm{Aut}(F)$ and consider $\psi\phi(\sigma) = (\psi\phi(\sigma)_X)_X = (F_1(\theta_{H(X)}^{-1})\sigma_{GH(X)}F_1(\theta_{H(X)}))$. As σ is an automorphism of functors, it commutes with the morphism $\theta_{H(X)}$, namely $\sigma_{GH(X)}F_1(\theta_{H(X)}) = F_1(\theta_{H(X)})\sigma_X$, and therefore $\psi\phi(\sigma)_X = \sigma_X \Rightarrow \psi\phi(\sigma)_X = \mathrm{id}_{\mathrm{Aut}(F)}$.

On the other hand, let $\epsilon \in \mathrm{Aut}(F_1)$. $\phi\psi(\epsilon) = (\phi\psi(\epsilon)_A)_A = F_1(\theta_A^{-1})\epsilon_{HG(A)}F_1(\theta_A)$. Using that ϵ commutes with θ_A, so $\epsilon_{HG(A)}F_1(\theta_A) = F_1(\theta_A)\epsilon_A$., and therefore $\phi\psi(\epsilon) = \epsilon \Rightarrow \phi\psi = \mathrm{id}_{\mathrm{Aut}(F_1)}$. This finalizes the proof of (b).

(a) Let's apply (b) to the profinite group $\pi = \varprojlim_{(A,a)\in J} \mathrm{Aut}_{\mathbf{C}}(A)$ and the functor H' constructed in Proposition 2.6. We proved that H' is an equivalence of categories, that yields F when composed with the forgetful functor F_1. Then $\pi \cong \mathrm{Aut}(F)$, and via this isomorphism we can identify H' and the previously defined $H : \mathbf{C} \to \mathrm{Aut}(F)\textbf{-sets}$ (it is easily observed from the proofs of Lemma 2.8 and (b) that the functor identification via the group morphisms defined yields the identity). Therefore, H is an equivalence of categories.

(c) Let $F' : \mathbf{C} \to \mathbf{sets}$ be a second fundamental functor. Then we have $\varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A,-) \cong F$, $\varinjlim_{J'} \mathrm{Mor}_{\mathbf{C}}(A,-) \cong F'$. Note that all the pairs $(A,a) \in J$ with the same A are isomorphic, so we can replace J by $J_0 \subset J$ with exactly one pair (A,a) for each A Galois; similarly, we replace J' by $J_0' \subset J'$ with exactly one pair (A,a) for each A Galois. Note here that the notion of Galois objects is independent of the fundamental functor.

Now, given $(A,a),(B,b) \in J_0$, $g : A \to B$ morphism, $\exists! \beta \in \mathrm{Aut}_{\mathbf{C}}(B)$ such that $F(\beta)(F(g)(a)) = b$. Then, $f = \beta g$ satisfies $F(f)(a) = b$ so $(A,a) \geq_f (B,b)$ in J_0, and this happens $\iff$ $(A,a') \geq_{f'} (B,b')$ in J_0', but the morphisms $f, f' : A \to B$, are not necessarily the same.

But it is true that $\forall \alpha \in \mathrm{Aut}_{\mathbf{C}}(A), \exists \gamma \in \mathrm{Aut}_{\mathbf{C}}(B)$ making the following diagram commute:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[d, "\gamma"] \\
A \arrow[r, "f'"] & B
\end{tikzcd}$$

Now mapping $\alpha \mapsto \gamma$ we obtain a system of morphisms between the finite nonempty groups $\mathrm{Aut}_{\mathbf{C}}(A)$, giving rise to a projective system. This limit is nonempty (endow the sets with discrete topology and use Proposition 1.3). This implies that we can make a simultaneous choice $(\alpha_A)_{(A,a) \in J_0}$ such that all the diagrams commute. This induces an isomorphism of functors $\varinjlim_{J_0} \mathrm{Mor}_{\mathbf{C}}(A,-) \cong \varinjlim_{J_0'} \mathrm{Mor}_{\mathbf{C}}(A,-)$, and so $F \cong F'$.

(d) Let $H' : \mathbf{C} \to \pi\text{-}\mathbf{sets}$ be an equivalence, and F' the composite of H' with the forgetful functor. Then $\pi \cong \mathrm{Aut}(F')$ by (b) and $F' \cong F$ by (c). The isomorphism between functors F, F' induces an isomorphism $\sigma : \mathrm{Aut}(F) \to \mathrm{Aut}(F')$ by letting $\epsilon' \in \mathrm{Aut}(F')$ correspond to ϵ: $\epsilon = \sigma\epsilon'\sigma^{-1}$. In conclusion, $\pi \cong \mathrm{Aut}(F)$ canonically.

□

2.7 Galois Theory for Fields

In this section we will develop the example already introduced in Example 2.3. The finite separable algebras over a field form a set. Then, the category of affine schemes over $\mathrm{Spec}(K)$ of the form $\mathrm{Spec}(B)$, where B is a free separable K-algebra is an essentially small Galois Category (we already proved in Example 2.3 that it is a Galois Category). We would like to give an explicit description of $\mathrm{Aut}(F)$ for this category. However, given an essentially small Galois Category $(\mathbf{C}, F)$, a priori we don't know how to calculate $\mathrm{Aut}(F)$ in terms of well-known groups. The only tool provided by Theorem 2.1 that can serve for this purpose is (d): If we are able to find a profinite group π such that $\mathbf{C}$ and π-**sets** are equivalent, then we have $\mathrm{Aut}(F) \cong \pi$.

Theorem 2.3. *Let K be a field and K_s its separable closure. Then, the category of affine schemes over K of the form* $\mathrm{Spec}(B)$, *with B a free separable K-algebra, is equivalent to the category of* $\mathrm{Gal}(K_s/K) -$ **sets**.

Proof. The category in the statement of the problem is antiequivalent to the category of finite free separable K-algebras (denoted from now on ${}_K\mathbf{SAlg}$), so it will be enough to prove that ${}_K\mathbf{SAlg}$ is antiequivalent to $\pi -$ **sets**, for $\pi = \mathrm{Gal}(K_s/K)$ the absolute Galois group of K.

Let's proceed to define the functors of the equivalence of categories. First, we define $F : {}_K\mathbf{SAlg} \to \pi -$ **sets**:

- **Objects**: Given B a finite free separable K-algebra, we define $F(B) = \mathrm{Alg}_K(B, K_s)$, that is the set of K-algebra morphisms from B to K_s. We should check that this is well defined, i.e., that $\mathrm{Alg}_K(B, K_s)$ is a π-set. Indeed, π acts on $\mathrm{Alg}_K(B, K_s)$ on the left by composition: Given $g \in \mathrm{Alg}_K(B, K_s)$, $\sigma \in \pi$, then also $\sigma \circ g \in \mathrm{Alg}_K(B, K_s)$. Using the decomposition of Lemma 2.1 (iv), we can write $B = \prod_{i=1}^{t} B_i$, where B_i is a finite separable field extension of K. Then, by the Galois correspondence, $B_i = K_s^{\pi_i}$, for $\pi_i \subset \pi$ an open subgroup of π. We claim that $\mathrm{Alg}_K(B, K_s) \cong \coprod_{i=1}^{t} \mathrm{Alg}_K(K_s^{\pi_i}, K_s)$. If we denote by $\{e_i\}_{i=1}^{t}$ the canonical basis of $B = \prod_{i=1}^{t} K_s^{\pi_i}$, we have that e_i is a root of $x(x-1)$, and therefore every morphism of K-algebras $f : B \to K_s$ maps e_i either to 1 or 0. At least one of the elements of the basis must be mapped to 1, as otherwise $f(\sum_{i=1}^{t} e_i) = f(1) = 1$ would yield a contradiction. On the other side, $f(e_i) = f(e_j) = 1$, also yields a contradiction $1 = f(e_i)f(e_j) = f(e_ie_j) = 0$. Therefore, $\forall i$ and $g \in \mathrm{Alg}(K^{\pi_i}, K_s)$, $\exists! g' \in \mathrm{Alg}(B, K_s)$ defined by $g'(b_1, \dots, b_t) = g(b_i)$. This defines a bijection $\mathrm{Alg}_K(B, K_s) \cong \coprod_{i=1}^{t} \mathrm{Alg}_K(K_s^{\pi_i}, K_s)$ which respects the π action, and so the claim is proved. Finally, note also that the map $\pi/\pi' \to \mathrm{Alg}(K_s^{\pi_i}, K_s)$ defined by $\sigma \mapsto \sigma|_{K_s^{\pi_i}}$ is a bijection which respects the π-actions. Therefore, we can identify $\mathrm{Alg}_K(B, K_s) \cong \coprod_{i=1}^{t} \pi/\pi_i$ as sets with an action of π. This shows that $\mathrm{Alg}_K(B, K_s)$ is a finite set, and, moreover, that the kernel of the action is $\bigcap_{i=1}^{t} \pi_i$, which is an open subgroup of π. Then, Proposition 1.8 tells us that the action of π on $\mathrm{Alg}_K(B, K_s)$ is continuous. With this we conclude that $\mathrm{Alg}_K(B, K_s)$ is indeed a π-set.

- **Morphisms**: Given a morphism of K-algebras $f : B \to C$, we define $F(f) : F(C) \to F(B)$ as $F(f)(g) = g \circ f$, for every $g \in \mathrm{Alg}_K(C, K_s)$. This is well defined: Indeed, its clear that it respects the composition and the identity so its functorial. Moreover, it is a morphism of π-**sets** as $\sigma F(f)(g) = \sigma \circ g \circ f = F(f)(\sigma g)$.

Now let's define the functor $G : \pi - \textbf{sets} \to {}_K\textbf{SAlg}$:

- **Objects**: Given E a π-set, we define $G(E) = \mathrm{Mor}_\pi(E, K_s)$. Note that the set $\mathrm{Mor}_\pi(E, K_s)$ has a natural K-algebra structure induced by the structure of K_s by pointwise multiplication. We have to check that it is finite and separable. Let $\{E_i\}_{i=1}^{n}$ be the set of orbits of E, $E \cong \coprod_{i=1}^{n} E_i$. Then its clear that $G(E) \cong \prod_{i=1}^{n} G(E_i)$. Let's study $G(E_i)$, i.e. how the functor G acts on transitive π-**sets**. We know by Proposition 1.8 that every transitive π-set is isomorphic to one of the form π/π', for a certain π' open subgroup of π. Every morphism of π-**sets** $g \in \mathrm{Mor}_\pi(\pi/\pi', K_s)$ is totally determined by $g(\pi') = a \in K_s$, as $g(\sigma\pi') = \sigma g(\pi') = \sigma(a)$. So an element $a \in K_s$ defines a morphism of π-**sets** $\pi/\pi' \to K_s$ if and only if $a \in K_s^{\pi'}$. In conclusion, given a π-set E, $E \cong \coprod_{i=1}^{n} \pi/\pi_i$, with π_i open subgroup of π, we have $G(E) \cong \prod_{i=1}^{n} K_s^{\pi_i}$, which is the product of finite separable extensions of K, and therefore a free separable K-algebra by Lemma 2.1.

- **Morphisms**: Given a morphism of π-**sets** $f : E \to D$, we define $G(f) : G(D) \to G(E)$ as $G(f)(g) = g \circ f$, for every $g \in \mathrm{Mor}_\pi(E, K_s)$.

We will now proceed to prove that the functors just defined are indeed an equivalence of categories. First, we define the morphism of functors $\theta : \mathrm{id}_{{}_K\textbf{SAlg}} \to GF$ by

$$\begin{aligned}
\theta_B : B &\longrightarrow GF(B) = \mathrm{Mor}_\pi(\mathrm{Alg}_K(B, K_s), K_s) \\
b &\longmapsto \qquad\qquad \theta_B(b) : \mathrm{Alg}_K(B, K_s) \longrightarrow K_s \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad g \longmapsto g(b)
\end{aligned}$$

For every $f : B \to C$, θ induces a diagram

$$\begin{tikzcd} B \arrow[r, "f"] \arrow[d, "\theta_B"] & C \arrow[d, "\theta_C"] \\ GF(B) \arrow[r, "GF(f)"] & GF(C) \end{tikzcd}$$

which is commutative, as $(\theta_C \circ f)(b)$ maps a morphism $g \in \mathrm{Mor}_\pi(\mathrm{Alg}_K(C, K_s), K_s)$ to $\theta_C(f(b))(g) = g(f(b))$ and, on the other hand, $(GF(f) \circ \theta_B)(b) = \theta_B(b) \circ F(f)$ maps a morphism $g \in \mathrm{Mor}_\pi(\mathrm{Alg}_K(C, K_s), K_s)$ to $\theta_B(b)(g \circ f) = g(f(b))$, so $(\theta_C \circ f) = (GF(f) \circ \theta_B)$ and the diagram commutes. It should be checked that θ_B is an isomorphism for every B, but this is true, as we can express θ_B as the composition of isomorphisms already defined above:

$$B \cong \prod_{i=1}^{t} K_i^{\pi_i} \cong \prod_{i=1}^{t} \mathrm{Mor}_\pi(\pi/\pi_i, K_s) \cong \mathrm{Mor}_\pi(\coprod_{i=1}^{t} \pi/\pi_i, K_s) \cong$$
$$\cong \mathrm{Mor}_\pi(\coprod_{i=1}^{t} \mathrm{Alg}(K_s^{\pi_i}, K_s), K_s) \cong \mathrm{Mor}_\pi(\mathrm{Alg}(\prod_{i=1}^{t} K_s^{\pi_i}, K_s), K_s)$$

Indeed, this chain of isomorphisms sends $b \mapsto (b_i) \mapsto (g_i)$, where each g_i satisfies $g_i(\pi_i) = b_i$, and the image of (g_i) in $\mathrm{Mor}_\pi(\coprod_{i=1}^t \mathrm{Alg}(K_s^{\pi_i}, K_s), K_s)$ is defined as follows. Take an element $f \in \mathrm{Alg}_K(K_s^{\pi_i}, K_s)$ defined by an element σ of the Galois group. Then, this f is mapped to $\sigma(b_i)$, which is equal to $f(b_i)$. This corresponds to θ_B when composed with the last isomorphism.

Similarly, we define the morphism of functors $\eta : \mathrm{id}_{\pi-\textbf{sets}} \to FG$ by

$$\begin{aligned} \eta_E : E \longrightarrow & FG(E) = \mathrm{Alg}_K(\mathrm{Mor}_\pi(E, K_s), K_s) \\ e \longmapsto & \qquad \eta_E(e) : \mathrm{Mor}_\pi(E, K_s) \longrightarrow K_s \\ & \qquad\qquad\qquad g \longmapsto g(e) \end{aligned}$$

Given $f : E \to D$, the morphism η yields a commutative diagram, as $(\eta_D \circ f)(e)(g) = g(f(e))$, which agrees with $(FG(f) \circ \eta_E)(e)(g) = (\eta_E(e) \circ G(f))(g) = \eta_E(e)(g \circ f) = g(f(e))$

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "\eta_E"] & D \arrow[d, "\eta_D"] \\ FG(E) \arrow[r, "FG(f)"] & FG(D) \end{tikzcd}$$

And the same argument as above proves that η_E is indeed an isomorphism: In particular, it is the composition of the following known isomorphisms:

$$E \cong \coprod_{i=1}^{n} \pi/\pi_i \cong \coprod_{i=1}^{n} \mathrm{Alg}(K_s^{\pi_i}, K_s) \cong \mathrm{Alg}(\prod_{i=1}^{n} K_s^{\pi_i}, K_s) \cong \mathrm{Alg}(\prod_{i=1}^{n} \mathrm{Mor}_\pi(\pi/\pi_i, K_s), K_s) \cong$$
$$\cong \mathrm{Alg}(\mathrm{Mor}_\pi(\coprod_{i=1}^{n} \pi/\pi_i, K_s), K_s) \cong \mathrm{Alg}(\mathrm{Mor}_\pi(E, K_s), K_s)$$

□

This theorem may be seen as a reformulation of the classical statement of Galois Theory for fields (i.e. there is a correspondence between finite separable extensions of a field K and open subgroups of its absolute Galois group). It should be noted that we haven't used at all the theory of Galois Categories to prove this equivalence, just classical Galois Theory. However, when we combine this result with Theorem 2.1, we obtain that $\mathrm{Gal}(K_s/K)$ is the unique profinite group (up to isomorphism) such that the category of free separable algebras over K is equivalent to the category of finite sets with a continuous action of the profinite group. This result is better that Theorem 2.3 alone, as it also has uniqueness, and is more concrete than Theorem 2.1 as it gives a more manageable description of the profinite group. The fact that the group is not unique, but unique up to isomorphism accounts here for the different choices of separable closures of K, which yield isomorphic Galois groups.

This example will be very relevant, as we will see that it is a particular case of the general theory for schemes that we want to develop, and, moreover, that we will need it to proof the general theory.

2.8 Functoriality

Theorem 2.1 gives rise to an assignation $(C, F) \mapsto \mathrm{Aut}(F)$ of a profinite group for every Galois category. To finish this section on Galois Categories, we will prove that this assignation is actually functorial, and some properties that arise from this fact.

Theorem 2.4. *Let $(\mathbf{C}, F)$ and $(\mathbf{C}', F')$ be two essentially small Galois categories, and $G : \mathbf{C} \to \mathbf{C}'$ a functor such that $F = F'G$. Let $H : \mathbf{C} \to \pi - \mathbf{sets}$ and $H' : \mathbf{C}' \to \pi' - \mathbf{sets}$, where π and π' denote $\mathrm{Aut}(F)$ and $\mathrm{Aut}(F')$. Then, there is a natural continuous group homomorphism $\pi' \to \pi$ such that the functor $G' : \pi - \mathbf{sets} \to \pi' - \mathbf{sets}$ that endows a π-set with the π' action induced by $\pi' \to \pi$ gives rise to a commutative diagram*

$$\begin{tikzcd}
\mathbf{C} \arrow[r, "G"] \arrow[d, "H"] & \mathbf{C}' \arrow[d, "H'"] \\
\pi - \mathbf{sets} \arrow[r, "G'"] & \pi' - \mathbf{sets}
\end{tikzcd}$$

Proof. Let's define a mapping $\mathrm{Aut}(F') \to \mathrm{Aut}(F)$ by

$$(\sigma'_Y)_{Y \in Ob(\mathbf{C}')} \mapsto (\sigma'_{G(X)})_{X \in Ob(\mathbf{C})}$$

$\sigma'_{G(X)}$ acts on $F_1(G(X)) = F(X)$, so it is a permutation of $F(X)$ and therefore the map is well defined, and it is clearly a group homomorphism. Moreover, let $U = \prod_{X \notin J} S_{F(X)} \times \prod_{X \in J} S'_{F(X)}$, for $\# J < \infty$ a basic open set of $\mathrm{Aut}(F)$, and $S'_{F(X)} \subset S_{F(X)}$. Its preimage is exactly the set $\sigma' \in \mathrm{Aut}(F')$ such that $\sigma'_{G(X)} \in S'_{F(X)}$, for $X \in J$, which is also a basic open set of $\mathrm{Aut}(F')$. Therefore, the map $\mathrm{Aut}(F') \to \mathrm{Aut}(F)$ just defined is indeed a morphism of profinite groups. We just have to check that G' makes the diagram commutative. When composed with the forgetful functor to **sets**, both $H'G$ and $G'H$ yield $F(X)$. Therefore it is enough to check that the action of an element of $\mathrm{Aut}(F')$ is the same in $H'G$ and $G'H$. Let $X \in Ob(\mathbf{C})$, $(\sigma'_Y)_{Y \in Ob(\mathbf{C}')} \in \mathrm{Aut}(F')$. Then, (σ'_Y) acts on $H'G(X)$ as the permutation $\sigma'_{G(X)}$, which agrees with the action on $G'H(X)$ by the definition of the map $\mathrm{Aut}(F') \to \mathrm{Aut}(F)$ above. □

Definition 2.6. We denote by **Gal** the category of small Galois Categories, that is defined as follows:

- **Objects**: Small Galois categories, that is, pairs $(\mathbf{C}, F)$ with $\mathbf{C}$ small.

- **Morphisms**: A morphism $(\mathbf{C}, F) \to (\mathbf{C}', F')$ is a functor $G : \mathbf{C} \to \mathbf{C}'$ satisfying $F = F'G$.

Proposition 2.9. The assignment $(\mathbf{C}, F) \mapsto \mathrm{Aut}(F)$ extends to a contravariant functor from **Gal** to the category of profinite groups.

Proof. Let's define a functor $J : \mathbf{Gal} \to \mathbf{Grp}_{Prof}$ that extends the assignment $J(\mathbf{C}, F) = \mathrm{Aut}(F)$. Let $G : (\mathbf{C}, F) \to (\mathbf{C}', F')$ be a morphism in **Gal**. Then, we are under the situation of Theorem 2.4, and so we have already seen that G induces a morphism of profinite groups $\mathrm{Aut}(F') \to \mathrm{Aut}(F)$, $(\sigma'_Y)_{Y\in Ob(\mathbf{C}')} \mapsto (\sigma'_{G(X)})_{X\in Ob(\mathbf{C})}$. Let's define $J(G)$ to be this morphism.

It is clear that this assignment sends the identity functor $\mathrm{id} : (\mathbf{C}, F) \to (\mathbf{C}, F)$ to the identity $\mathrm{id} : \mathrm{Aut}(F) \to \mathrm{Aut}(F)$. Moreover, given $(\mathbf{C}'', F'')$ another object of **Gal**, and a morphism $G' : (\mathbf{C}', F') \to (\mathbf{C}'', F'')$, we have

$$J(G' \circ G)((\sigma''_Z)_{Z\in Ob(\mathbf{C}'')}) = (\sigma''_{G'G(X)})_{X\in Ob(\mathbf{C})} = J(G) \circ J(G')((\sigma''_Z)_{Z\in Ob(\mathbf{C}'')})$$

Therefore J defines a contravariant functor from **Gal** to the category of profinite groups. □

Example 2.8. Let K' be a field and K a subfield. Let $\mathbf{C}$ be the category of affine schemes over K of the form $\mathrm{Spec}(B)$, where B is a free separable K-algebra. Similarly let $\mathbf{C}'$ be the category of affine schemes $\mathrm{Spec}(B)$, with B a free separable K'-algebra. Let $F : \mathbf{C} \to {}_K\mathbf{SAlg} \to \mathbf{sets}$, where the last functor is $\mathrm{Alg}_K(-, K_s)$, and similarly let $F' : \mathbf{C}' \to {}_{K'}\mathbf{SAlg} \to \mathbf{sets}$, with $\mathrm{Alg}_{K'}(-, K'_s)$ as second functor. The functor ${}_K\mathbf{SAlg} \to {}_{K'}\mathbf{SAlg}$ sending $A \mapsto A \otimes_K K'$ induces a functor $G : \mathbf{C} \to \mathbf{C}'$, which satisfies $F = F'G$. Therefore this gives rise to a continuous group homomorphism $\mathrm{Gal}(K'_s/K') \to \mathrm{Gal}(K_s/K)$, which is the map restricting the action of $\mathrm{Gal}(K'_s/K')$ to K_s, which is a subfield of K'_s.

Proposition 2.10. Let $\pi' \to \pi$ be a morphism of profinite groups, and $G' : \pi - \mathbf{sets} \to \pi' - \mathbf{sets}$ the functor induced by endowing a π-set with the π' action induced by $\pi' \to \pi$. Then,

i) $\pi' \to \pi$ is surjective if and only if G' sends connected π-sets to connected π'-sets.

ii) $\pi' \to \pi$ is injective if and only if for every connected object X' of π'-**sets** there is an object X of π-**sets** and a connected component Y' of $G'(X)$ such that there is a π'-homomorphism $Y' \to X'$

Proof. Let's denote by f the morphism of profinite groups $\pi' \to \pi$. Let's remind that G' does not change the underlying set, just the action. So we will denote without distinction the elements of E and $G'(E)$. It should also be reminded that connected objects in the category of π-**sets** are the transitive π-sets.

i) $\boxed{\Rightarrow}$ Let E be a connected π-set, and $e \in E$. Then, $\forall e' \in E\ \exists \sigma \in \pi$ such that $\sigma e = e'$. By surjectivity of f, $\exists \sigma' \in \pi'$ such that $f(\sigma') = \sigma$. Therefore $\sigma' e = f(\sigma')e = \sigma e = e'$, which proves that $G'(E)$ is transitive.

$\boxed{\Leftarrow}$ Suppose that f is not surjective, that is, $\exists \sigma \in \pi$ such that $f^{-1}(\sigma) = \varnothing$, and let $\{\pi_i\}$ be the set of open subgroups of π. These groups are in particular closed, and then, so are $\sigma\pi_i$, for every $\sigma \in \pi$. Therefore, the sets $f^{-1}(\sigma\pi_i)$ are also closed. By Proposition 1.7, as f is not surjective, $\bigcap_i f^{-1}(\sigma\pi_i) = \varnothing$. But as π' is profinite and therefore compact, a finite number of these sets will do to intersect to the empty set. Let $\sigma\pi_1, \dots, \sigma\pi_n$ be these sets. Take an open subgroup $\tilde{\pi} \subset \pi$ such that $\tilde{\pi} \geq \pi_i$ for every $i = 1, \dots, n$ (that is $\pi_i \subseteq \tilde{\pi}$). As the connected π-set $\pi/\tilde{\pi}$ is sent by G to a connected π'-set, $\exists \sigma' \in \pi'$ such that $f(\sigma')\tilde{\pi} = \sigma\tilde{\pi}$, and so $f(\sigma')\pi_i = \sigma\pi_i$, for $i = 1, \dots, n$, which is a contradiction.

ii) $\boxed{\Leftarrow}$ Suppose that $\exists \sigma_1, \sigma_2 \in \pi'$ such that $f(\sigma_1) = f(\sigma_2)$. Take π'' an open subgroup of π, and denote $X' = \pi/\pi''$. By hypothesis, there is an Y' connected π'-set and a morphism $\phi : Y' \to \pi'/\pi''$. Take

$e \in Y'$. Without loss of generality we can assume that $\phi(e) = \pi''$. If $f(\sigma_1)e = f(\sigma_2)e$, applying ϕ we get that $\sigma_1^{-1}\sigma_2 \in \pi''$. As this holds for every open π'', Proposition 1.7 tells us that $\sigma_1 = \sigma_2$.

$\boxed{\Rightarrow}$ If $\pi' \to \pi$ is injective, we can consider π' a subgroup of π. For every open subgroup of π', $\pi'' \subset \pi'$, $\exists \tilde{\pi}$ open subgroup of π such that $\pi'' = \pi \cap \tilde{\pi}$. The subset of $\pi/\tilde{\pi}$ given by $Y' = f(\pi')\tilde{\pi}$ is a connected component of $G'(\pi/\tilde{\pi})$. Then we can easily define a map $f(\sigma)\pi \mapsto \sigma\pi''$. This morphism of π'-sets is well defined, as $f(\sigma_1)^{-1}f(\sigma_2) \in \tilde{\pi} \Rightarrow \sigma_1^{-1}\sigma_2 \in \tilde{\pi} \cap \pi' = \pi''$.

□

3. Projective modules and projective algebras

In this section we introduce and treat the main properties of projective modules and algebras, and also the notion of projective separable algebras. This concepts are key, as we will see later that, in the affine setting, finite and locally free morphisms of schemes correspond to finite projective algebras in the ring language, and finite étale morphisms of schemes correspond to projective separable algebras. This chapter should be regarded as something like the affine characterization of finite étale coverings.

3.1 Projective modules

Definition 3.1. An A-module P is called *projective* if the functor $\mathrm{Hom}_A(P, -)$ on the category of A-modules is exact. Recall that this means that for every exact sequence $M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2$, the induced sequence

$$\mathrm{Hom}_A(P, M_0) \xrightarrow{f_1 \circ -} \mathrm{Hom}_A(P, M_1) \xrightarrow{f_2 \circ -} \mathrm{Hom}_A(P, M_2)$$

is exact as an A-module sequence.

Now we will proceed to give some equivalent characterizations of the concept of projective A-module.

Definition 3.2. An exact sequence of A-modules $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0$ *splits* if there exists an isomorphism of A-modules $\theta : M_1 \cong M_0 \oplus M_2$ making the following diagram commutative

$$\begin{tikzcd}
0 \arrow[r] & M_0 \arrow[r, "f"] \arrow[d, "\mathrm{id}"] & M_1 \arrow[r, "g"] \arrow[d, "\theta"] & M_2 \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & M_0 \arrow[r] & M_0 \oplus M_2 \arrow[r] & M_2 \arrow[r] & 0
\end{tikzcd}$$

Lemma 3.1. The following assertions are equivalent:

i) $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2 \to 0$ splits.

ii) $\exists$ an A-linear map $h : M_1 \to M_0$ such that $M_0 \xrightarrow{f} M_1 \xrightarrow{h} M_0$ is the identity map.

iii) $\exists$ an A-linear map $h' : M_2 \to M_1$ such that $M_2 \xrightarrow{h'} M_1 \xrightarrow{g} M_2$ is the identity map.

Proof. $\boxed{(i) \iff (ii)}$ Let $\theta : M_1 \cong M_0 \oplus M_2$ denote the isomorphism. Then, given $p : M_0 \oplus M_2 \to M_0$ the projection map, $p \circ \theta : M_1 \to M_0$ yields the identity when composed with f, by commutativity of the diagram

$$\begin{tikzcd}
M_0 \arrow[r, "f"] \arrow[d, "\mathrm{id}"] & M_1 \arrow[d, "\theta"] & \\
M_0 \arrow[r] \arrow[rr, bend right, "\mathrm{id}"'] & M_0 \oplus M_2 \arrow[r, "p"] & M_0
\end{tikzcd}$$

Reciprocally, given the morphism $h : M_1 \to M_0$, let's build the map $\phi : M_1 \to M_0 \oplus M_2$ sending

$x \mapsto (h(x), g(x))$. It's clear that the map ϕ yields the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & M_0 \arrow[r, "f"] \arrow[d, "\mathrm{id}"] & M_1 \arrow[r, "g"] \arrow[d, "\phi"] & M_2 \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & M_0 \arrow[r] & M_0 \oplus M_2 \arrow[r] & M_2 \arrow[r] & 0
\end{tikzcd}$$

so it's only left to check that ϕ is an isomorphism to prove that the sequence splits.

Indeed, let $(x, y) \in M_0 \oplus M_2$. By the surjectivity of g, $\exists a \in M_1$ such that $g(a) = y$. Then take $b = a - f(h(a)) + f(x)$, and we have that $g(b) = y$, $h(b) = h(a) - h(a) + h(f(x)) = x$, so ϕ is surjective. Now suppose that $h(x) = h(y)$, $g(x) = g(y)$. By the fact that $M_1/M_0 \cong M_2$, $g(x) = g(y) \Rightarrow x = y + f(z)$, for a certain $z \in M_0$. Now, applying h, we have $h(x) = h(y) + hf(z) \Rightarrow z = hf(z) = 0 \Rightarrow f(z) = 0$, and so $x = y$.

$\boxed{(i) \iff (iii)}$ Given the isomorphism $\theta : M_1 \cong M_0 \oplus M_2$, consider the natural inclusion map $i : M_2 \to M_0 \oplus M_2$, $x \mapsto (0, x)$. The composition with the projection $M_0 \oplus M_2 \to M_2$ yields the identity, and so we have the following commutative diagram

$$\begin{tikzcd}
 & M_1 \arrow[r, "g"] & M_2 \arrow[d, "\mathrm{id}"] \\
M_2 \arrow[r, "i"] \arrow[rr, bend right, "\mathrm{id}"'] & M_0 \oplus M_2 \arrow[r, "p"] \arrow[u, "\theta^{-1}"] & M_2
\end{tikzcd}$$

and, in conclusion, $h' := \theta^{-1} \circ i$ is the desired morphism.

Reciprocally, consider the morphism $\phi : M_0 \oplus M_2 \to M_1$ given by $(x, y) \mapsto f(x) + h'(y)$. It is clearly satisfied that the diagram

$$\begin{tikzcd}
0 \arrow[r] & M_0 \arrow[r, "f"] \arrow[d, "\mathrm{id}"] & M_1 \arrow[r, "g"] & M_2 \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & M_0 \arrow[r] & M_0 \oplus M_2 \arrow[r] \arrow[u, "\phi"] & M_2 \arrow[r] & 0
\end{tikzcd}$$

is commutative, so it will be enough to check that ϕ is an isomorphism. Note that every element of M_1 can be written as $h'g(y) + a$, with $a \in f(M_0)$, because $M_1 \cong M_2/M_0$. Then, given $y \in M_1$, we can write $y = h'g(y) + f(x)$, and $\phi(x, g(y)) = y$, so ϕ is surjective.

On the other side, suppose that we have $\phi(x_1, y_1) = \phi(x_2, y_2)$. Applying g, we get $y_1 = y_2$. Then, $h'(y_1) = h'(y_2)$, and so $f(x_1) = f(x_2)$, and finally, by injectivity of f, we have $x_1 = x_2$, and so ϕ is injective. □

Proposition 3.1. Let A be a ring and P an A-module. The following statements are equivalent.

i) P is projective.

ii) The functor $\mathrm{Hom}_A(P, -)$ is right-exact.

iii) Every exact sequence $0 \to M_0 \to M_1 \to P \to 0$ splits.

iv) $\exists$ an A-module Q such that $P \oplus Q$ is free.

Proof. $\boxed{(i) \Rightarrow (ii)}$ is trivial, as if the Hom functor is exact, it is in particular right-exact.

$\boxed{(ii) \Rightarrow (iii)}$ The fact that $\operatorname{Hom}_A(P, -)$ is right-exact means that for every A-linear map $g : M \to N$ which is surjective, and $\forall f : P \to N$, $\exists$ an A-linear map $h : P \to M$ that makes commutative the diagram

$$\begin{tikzcd} & P \arrow[dl, dotted, "h"'] \arrow[d, "f"] & \\ M \arrow[r, "g"] & N \arrow[r] & 0 \end{tikzcd}$$

Therefore, given an exact sequence $0 \to M_0 \to M_1 \to P \to 0$, we can take $M = M_1$, $N = P$, $f = \mathrm{id}$ and $g : M_1 \to P$, we see that $\exists h$ satisfying characterization (iii) of Lemma 3.1, and so the sequence $0 \to M_0 \to M_1 \to P \to 0$ splits.

$\boxed{(iii) \Rightarrow (iv)}$ Let's map a free module to a set of generators of P, $\varphi : \bigoplus_{i \in I} A \to P$, which is a surjective map. Therefore, $0 \to \ker \varphi \to \bigoplus_{i \in I} A \xrightarrow{\varphi} P \to 0$ splits, and so $P \oplus \ker \varphi \cong \bigoplus_{i \in I} A$, and P is a direct summand of a free A-module.

$\boxed{(iv) \Rightarrow (i)}$ Suppose that we have $P \cong \bigoplus_{i \in I} P_i$. Using $\operatorname{Hom}_A(P, M) \cong \prod_{i \in I} \operatorname{Hom}_A(P_i, M)$ (universal property of sums), it is immediate that the functor $\operatorname{Hom}_A(P, -)$ is exact if and only if $\operatorname{Hom}_A(P_i, -)$ is exact for all $i \in I$. Therefore, P is projective $\iff$ P_i projective $\forall i$.

Now, first of all note that A is a projective A-module, as $\operatorname{Hom}_A(A, M) \cong M$, and through this isomorphism the functor $\operatorname{Hom}_A(A, M)$ can be seen as the identity, so it is exact. In consequence, free A-modules are projective, and direct summands of free A-modules are also projetive. □

Observation 3.1. If P a finitely generated module over a ring A, then P is projective $\iff$ $\exists Q$ A-module such that $P \oplus Q \cong A^n$ for a certain Q which is finitely generated. This is immediate because if P is projective the sequence $0 \to \ker \phi \to A^n \to P \to 0$ splits, and so we have $P \oplus Q \cong A^n$, where $Q := \ker \phi$. Q must be finitely generated as both P, A^n are finitely generated.

Observation 3.2. Note that every projective module is also flat. Indeed, A is flat as an A-module, and a sum of modules is flat $\iff$ each summand is flat. Therefore, free modules are flat and direct summands of free modules (that is, projective modules) are also flat.

Example 3.1. Let's see some examples of projective modules:

i) Free modules are projective modules. For example, if $A = k$ is a field, every A-module (that is, every k-vector space) is free, and therefore projective.

Another particular case is the case of principal ideal domains: Every ideal is isomorphic to A as an A-module, and so every ideal is free and therefore projective.

ii) **Hereditary rings:**

Definition 3.3. A ring is called *hereditary* if every ideal is projective.

Proposition 3.2. In a hereditary ring every submodule of a free A-module is isomorphic to a direct sum of ideals of A. In particular, every projective module is the sum of ideals of A.

Proof. Let M be a submodule of a free A-module. Let's consider the maps f_i defined as

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] \arrow[rr, bend right, "f_i"'] & \bigoplus_{i\in I} A \arrow[r, "\pi_i"] & A \end{tikzcd}$$

. $f_i(M)$ is an ideal of A, that we can denote as J_i. As J_i is projective, $\exists h_i : J_i \to M$ such that $f_i \circ h_i = \mathrm{id}_{J_i}$. Then, by the universal property of the direct sum, there is a map $g_i : \bigoplus_{i\in I} J_i \to M$ corresponding to the set of maps $(0, \dots, 0, h_i, 0, \dots, 0)$, satisfying $f_j \circ g_i = \delta_{ij}$. Then, there is a map $\bigoplus_{i\in I} J_i \to M$, $(x_i)_{i\in I} \mapsto \sum_{i\in I} g_i(x_i)$, and this guarantees that $M \mapsto \bigoplus_{i\in I} J_i$ is surjective, and therefore an isomorphism. □

Proposition 3.3. Dedekind domains are hereditary rings.

Proof. In a Dedekind domain A, every non-zero fractional ideal of A is invertible ([1], Theorem 9.8). Therefore, let I be an ideal of A, and we know that $(A : I)I = A$, so $\exists x_1, \dots x_n \in I$, $y_1, \dots y_n \in (A : I)$ such that $\sum_{i=1}^n x_i y_i = 1$. Now consider the maps $\varphi : I \to A^n$, $x \mapsto (xy_i)_{i=1}^n$, and $\psi : A^n \to I$, $(a_i)_{i=1}^n \mapsto \sum_{a_i x_i}$. Then, $\psi \circ \varphi = \mathrm{id}_I$, and so the sequence $0 \to \ker\psi \to A^n \xrightarrow{\psi} I \to 0$ splits, and so I is a direct summand of a free module $\Rightarrow$ I is projective. □

This gives us the first particular example of a projective module that is not free: An ideal in a Dedekind domain that is not principal. For instance, the typical example of this case is the ideal $(2, 1 + \sqrt{-5})$ in the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$.

iii) Let $A = A_1 \times A_2$ as rings. Then, A_1 is a projective A-module, induced by the projection map $p_1 : A \to A_1$. Indeed, as $A_1 \oplus A_2 \cong A_1 \times A_2 = A$, A_1 is a direct summand of a free A-module. Clearly A_1 itself is not free in the general case (for example take $A_1 = A_2$).

3.2 Local characterization of projective modules

After introducing the concept of projective modules, we will see how finitely generated projective modules can be locally characterized.

Lemma 3.2. If A is a local ring, every finitely generated projective A-module is free.

Proof. Let A be a local ring, with maximal ideal $\mathfrak{m}$. Let P be a finitely generated projective A-module. Take $x_1, \dots, x_n \in P$ satisfying that $x_i \otimes 1$ form a base of the $A/\mathfrak{m}$ vector space $P \otimes A/\mathfrak{m}$. Then, the map $f : A^n \to P$, $e_i \mapsto x_i$ satisfies that $f \otimes \mathrm{id}_{A/\mathfrak{m}} : (A/\mathfrak{m})^n \to P \otimes A/\mathfrak{m}$ is an isomorphism (using surjectivity and that they have the same dimension).

Take $M = \mathrm{coker}(f)$. As tensoring is right-exact, we have that $A^n \otimes A/\mathfrak{m} \xrightarrow{f\otimes\mathrm{id}_{A/\mathfrak{m}}} P \otimes A/\mathfrak{m} \to M \otimes A/\mathfrak{m} \to 0$ is exact. But the fact that $f \otimes \mathrm{id}_{A/\mathfrak{m}}$ is an isomorphism implies that $0 = M \otimes A/\mathfrak{m} \cong M/\mathfrak{m}M$. In conclusion, $M = \mathfrak{m}M$, and so by Nakayama's lemma we have $M = 0$. Therefore f is surjective.

Therefore, we have the exact sequence $0 \to \ker f \to A^n \to P \to 0$. As P is projective, the sequence splits, and therefore there is an isomorphism $A^n \cong P \oplus \ker f$, and in particular $\ker f$ is finitely generated. Then, $A^n \otimes A/\mathfrak{m} \cong (P \otimes A/\mathfrak{m}) \oplus (\ker f \otimes A/\mathfrak{m})$, and so $\ker f/\mathfrak{m}\ker f = 0$. Using Nakayama's lemma again, we conclude that $\ker f = 0$ and so f is an isomorphism, and P is free. □

Definition 3.4. We say that an A-module M is *finitely presented* if $\exists$ an exact sequence $A^m \to A^n \to M \to 0$.

Lemma 3.3. Let M, N be A-modules, and M finitely presented. Let $S \subset A$ be a multiplicatively closed subset of S. Then, the map

$$\begin{aligned} S^{-1}\mathrm{Hom}_A(M,N) &\longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N) \\ h/s &\longmapsto \quad h' : S^{-1}M \longrightarrow S^{-1}N \\ & \qquad\qquad\qquad \frac{a}{t} \longmapsto \frac{h(a)}{ts} \end{aligned}$$

is an isomorphism of $S^{-1}A$-modules.

Proof. Note that we have the maps $\phi : \mathrm{Hom}_{S^{-1}A}(S^{-1}A, S^{-1}N) \to S^{-1}N$, $\phi(f) = f(1)$ and $\psi : S^{-1}\mathrm{Hom}_A(A,N) \to S^{-1}N$, $\psi(f/s) = f(1)/s$, which are isomorphisms of A-modules. The composition $\phi^{-1} \circ \psi : S^{-1}\mathrm{Hom}_A(A,N) \to \mathrm{Hom}_{S^{-1}A}(S^{-1}A, S^{-1}N)$ yields the natural map of the statement, for the case $M = A$. So for the case $M = A$, the map of the statement is an isomorphism. Taking into account that $\mathrm{Hom}_A(A^n, N) \cong \bigoplus_{i=1}^n \mathrm{Hom}(A,N)$, and $\mathrm{Hom}_{S^{-1}A}((S^{-1}A)^n, S^{-1}N) \cong \bigoplus_{i=1}^n \mathrm{Hom}_{S^{-1}A}(S^{-1}A, S^{-1}N)$, the result also holds for free (and finitely generated) A-modules.

Now let's deal with the case where M is finitely presented: We can write the following exact sequence: $A^m \xrightarrow{f} A^n \xrightarrow{g} M \to 0$. Now using that $\mathrm{Hom}_A(-,N)$ transforms a right exact sequence into a left exact one, and that S^{-1} is an exact functor, we have the following exact sequences:

$$0 \to S^{-1}\mathrm{Hom}_A(M,N) \xrightarrow{S^{-1}\overline{g}} S^{-1}\mathrm{Hom}_A(A^n,N) \xrightarrow{S^{-1}\overline{f}} S^{-1}\mathrm{Hom}_A(A^m,N)$$

$$0 \to \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N) \xrightarrow{\overline{S^{-1}g}} \mathrm{Hom}_{S^{-1}A}((S^{-1}A)^n, S^{-1}N) \xrightarrow{\overline{S^{-1}f}} \mathrm{Hom}_{S^{-1}A}((S^{-1}A)^m, S^{-1}N)$$

Where we have denoted $S^{-1}\overline{h} := \frac{-\circ h}{1}$ and $\overline{S^{-1}h} := - \circ \frac{h}{1}$.

Given a morphism $h : M' \to M$, the natural map of the statement of the lemma induces a commutative diagram

$$\begin{tikzcd}
S^{-1}\mathrm{Hom}_A(M,N) \arrow[r, "S^{-1}\overline{h}"] \arrow[d] & S^{-1}\mathrm{Hom}_A(M',N) \arrow[d] \\
\mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N) \arrow[r, "\overline{S^{-1}h}"] & \mathrm{Hom}_{S^{-1}A}(S^{-1}M', S^{-1}N)
\end{tikzcd}$$

And, in consequence, we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & S^{-1}\mathrm{Hom}_A(M,N) \arrow[r, "S^{-1}\overline{g}"] \arrow[d] & S^{-1}\mathrm{Hom}_A(A^n,N) \arrow[r, "S^{-1}\overline{f}"] \arrow[d] & S^{-1}\mathrm{Hom}_A(A^m,N) \arrow[d] \\
0 \arrow[r] & \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N) \arrow[r, "\overline{S^{-1}g}"] & \mathrm{Hom}_{S^{-1}A}((S^{-1}A)^n, S^{-1}N) \arrow[r, "\overline{S^{-1}f}"] & \mathrm{Hom}_{S^{-1}A}((S^{-1}A)^m, S^{-1}N)
\end{tikzcd}$$

Now, as the vertical maps are isomorphisms in the free case, the remaining vertical map (the first one, for the case of M) has to be an isomorphism too. □

Lemma 3.4. Let $\{f_i\}_{i\in I} \subseteq A$, with $\sum_{i \in I} Af_i = A$. Let M be an A-module.

i) If $M_{f_i} = 0 \ \forall i \in I$, then $M = 0$.

ii) If M_{f_i} is a finitely generated A_{f_i}-module $\forall i \in I$; then M is a finitely generated A-module.

Proof. i) As $\sum_{i\in I} Af_i = A$, then $\exists f_1, \dots, f_n$, $f_i \in \{f_\alpha\}_{\alpha\in I}$, and $a_i \in A$, $i \in \{1, \dots, n\}$, such that $\sum_{i=1}^n a_i f_i = 1$. Let $x \in M$. As $M_{f_i} = 0$, $\exists m_1, \dots, m_n$ such that $f_i^{m_i} x = 0$. Now let $\mathrm{m} = \sum_{i=1}^n m_i - n + 1$. We have $(\sum_{i=1}^n a_i f_i)^m = 1$, and expanding the sum we see that each summand is of the form $\prod_{i=1}^n f_i^{d_i}$, with $\sum d_i = m$. Therefore, there is at least one i such that $d_i \geq m_i$, and that happens for every term of the sum. In conclusion, we have $0 = x(\sum_{i=1}^n a_i f_i)^m = x$. As this holds $\forall x \in M$, we conclude that $M = 0$.

ii) Let $y \in M$, $\{f_i\}_{i=1}^n$ chosen as before. Then, for every $i = 1, \dots, n$, we have the expression $\frac{y}{1} = \sum_{j=1}^{t_i} x_{ij} \frac{a_{ij}}{f_i^{m_{ij}}}$ in M_{f_i}, where the set $\left\{ \frac{x_{ij}}{f_i^{m_{ij}}} \right\}_{j=1}^{t_i}$ is a set of generators of M_{f_i}. Taking $M_i = \max_j(m_{ij})$, we can write it as $\frac{y}{1} = \frac{1}{f^{M_i} \sum_{j=1}^{t_i} x_{ij}} \frac{a_{ij}}{f_i^{M_i - m_{ij}}}$. This implies that $\exists K_i$ such that $(f_i^{M_i} y - \sum_{j=1}^{t_i} x_{ij} a_{ij} f_i^{M_i - m_{ij}}) f_i^{K_i} = 0$. If we rename $M_i' := M_i + K_i$ we get the following expression

$$f_i^{M_i'} y = \sum_{j=1}^{t_i} x_{ij} a_{ij} f_i^{M_i' - m_{ij}}$$

Let's remind that, if $(f_i)_{i=1}^n = (1)$, then for arbitrary exponents $(\alpha_i)_{i=1}^n$, $\alpha_i \geq 0$, we have that $(f_i^{\alpha_i})_{i=1}^n = (1)$ (see the proof of part (i)). Therefore, $\exists b_1, \dots, b_n$ such that $\sum_{i=1}^n b_i f_i^{M_i'} = 1$. Then, $y = \sum_{i=1}^n b_i \sum_{j=1}^{t_i} x_{ij} a_{ij} f_i^{M_i' - m_{ij}}$. This proves that the set $(x_{ij})_{i,j}$ generates M, and as it is a finite set, M is finitely generated.

□

Now we are ready to prove the theorem giving the local characterization of finitely generated projective modules.

Theorem 3.1. *Let A be a ring, and P an A-module. The following statements are equivalent:*

i) P is a finitely generated projective A-module.

ii) P is finitely presented, and $P_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module for every $\mathfrak{m}$ maximal ideal of A.

iii) $\exists (f_i)_{i\in I}$ elements of A with $\sum_{i\in I} Af_i = A$ such that $\forall i \in I$, P_{f_i} is free of finite rank as an A_{f_i}-module.

Proof. $\boxed{(i) \Rightarrow (ii)}$ By Observation 3.1, there exists a finitely generated A-module Q such that $P \oplus Q \cong A^n$. This implies that P is finitely presented. Moreover, given a maximal ideal $\mathfrak{m}$, tensoring the isomorphism $P \oplus Q \cong A^n$ with $A_\mathfrak{m}$ we get $P_\mathfrak{m} \oplus Q_\mathfrak{m} \cong A_\mathfrak{m}^n \Rightarrow P_\mathfrak{m}$ is a finitely generated projective $A_\mathfrak{m}$-module. As $A_\mathfrak{m}$ is a local ring, $P_\mathfrak{m}$ is free by Lemma 3.2.

$\boxed{(ii) \Rightarrow (iii)}$ Let's fix a maximal ideal $\mathfrak{m}$, and let's denote $h : P_\mathfrak{m} \cong A_\mathfrak{m}^n$ and $g = h^{-1}$. As both A^n, P are finitely presented, therefore using Lemma 3.3 we have that $g = g'/s$, $h = h'/t$, where $h' : P \to A^n$, $g' : A^n \to P$ and $s, t \in A \setminus \mathfrak{m}$. Then,

$$g \circ h = \mathrm{id}_{P_\mathfrak{m}} \Rightarrow \exists u \in A \setminus \mathfrak{m} \text{ such that } u(g' \circ h' - st\mathrm{id}_P) = 0$$
$$h \circ g = \mathrm{id}_{(A_\mathfrak{m})^n} \Rightarrow \exists v \in A \setminus \mathfrak{m} \text{ such that } v(h' \circ g' - st\mathrm{id}_{A^n}) = 0$$

Let $f = stuv \in A \setminus \mathfrak{m}$. Note that we can write $g'' := tuvg'/f = g'/s$, $h'' := suvh'/f = h'/t$. These maps are inverse to each other, and are defined between the modules A_f^n and P_f, so $P_f \cong A_f^n$. Varying $\mathfrak{m}$, we obtain the desired collection $(f_i)_{i\in I}$, where in this case I is the set of maximal ideals of A. It's clear that the set $(f_i)_{i\in I}$ generates A, because for every maximal ideal $\mathfrak{m}$ of A, the corresponding element $f_\mathfrak{m}$ doesn't belong to A, so the ideal generated by $(f_i)_{i\in I}$ cannot be a subset of any maximal, and therefore it must be the whole ring.

$\boxed{(iii) \Rightarrow (i)}$ Note that we can select a finite subset of the set $(f_i)_{i\in I}$, denoted $f_1, \dots, f_n$ such that $\sum_{i=1}^n a_i f_i = 1$. Consider for each $i = 1, \dots, n$, an isomorphism $g_i : A_{f_i}^{n(i)} \to P_{f_i}$. Note that we can choose g_i mapping the basic elements into the image of P in P_{f_i} (as the image of P in P_{f_i} generates P_{f_i} as A_{f_i}-module). Then, g_i is induced by a certain $g_i' : A^{n(i)} \to P$, and the set of maps g_i' combine to form a map $g' : A^{\sum_{i=1}^n n(i)} \to P$.

As each $g_i' \otimes \mathrm{id}_{A_{f_i}}$ is surjective (because it is an isomorphism), we have that $g' \otimes \mathrm{id}_{A_{f_i}}$ is surjective. Then, the cokernel M of g' satisfies that $M_{f_i} = 0\ \forall i$, and using Lemma 3.4 (i), we conclude that $M = 0$.

Now we will proceed to prove that P is finitely presented. Note that $g' \otimes \mathrm{id}_{A_{f_i}}$ has kernel $A_{f_i}^{\sum_{j\neq i} n(j)}$, as we have a sequence $0 \to \ker(g' \otimes \mathrm{id}_{A_{f_i}}) \to A_{f_i}^{\sum_{i=1}^n n(j)} \to P_{f_i} \to 0$ that splits because P_{f_i} are free and therefore projective, and so $A_{f_i}^{\sum_{j\neq i} n(j)} \cong \ker(g' \otimes \mathrm{id}_{A_{f_i}})$. So the kernel of $g' \otimes \mathrm{id}_{A_{f_i}}$ is finitely generated $\forall i$, and therefore by Lemma 3.4 (ii) we conclude that P is finitely presented.

Suppose that we have a surjective A-lineal map $h : M \to N$, and consider the map $\mathrm{Hom}_A(P, M) \xrightarrow{h\circ -} \mathrm{Hom}_A(P, N)$. Tensoring this map with A_{f_i}, and recalling that we are allowed to use Lemma 3.3 as P is finitely presented, we have the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Hom}_A(P, M) \otimes A_{f_i} \arrow[r, "h\otimes \mathrm{id}_{A_{f_i}} \circ -"] \arrow[d, "\cong"] & \mathrm{Hom}_A(P, N) \otimes A_{f_i} \arrow[d, "\cong"] \\
\mathrm{Hom}_{A_{f_i}}(P_{f_i}, M_{f_i}) \arrow[r, "h_{f_i} \circ -"] & \mathrm{Hom}_{A_{f_i}}(P_{f_i}, N_{f_i})
\end{tikzcd}$$

Where we have denoted h_{f_i} the A_{f_i}-linear natural map $M_{f_i} \to N_{f_i}$ induced by h. As h is surjective, h_{f_i} is also surjective, and therefore the map $h_{f_i} \circ -$ is surjective because P_{f_i} is projective. As the vertical maps of the commutative diagram are isomorphisms, also $h \otimes \mathrm{id}_{A_{f_i}} \circ -$ is surjective. Therefore, applying Lemma 3.4 (a) to the cokernel of the map $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N)$ we get that it is also surjective, and therefore P is projective, by the second characterization of Proposition 3.1. □

Observation 3.3. Let P be a finitely generated projective module over a ring A. We can reformulate (iii) of the last theorem in the scheme-theoretic language, as follows: There exists an open cover of $\mathrm{Spec}(A)$ (namely $X_{f_i} \cong \mathrm{Spec}(A_{f_i})$, ranging over a set I), such that the sheaf associated to P on $\mathrm{Spec}(A)$ satisfies $\Gamma(P, X_{f_i}) \cong P_{f_i} \cong A_{f_i}^{n(i)}$.

Therefore, if we choose a prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$, and $f_i \notin \mathfrak{p}$, we have $P_\mathfrak{p} \cong P_{f_i} \otimes (A_{f_i})_{\overline{\mathfrak{p}}} \cong A_\mathfrak{p}^{n(i)}$. So it makes sense to talk about the rank of $P_\mathfrak{p}$ for each $\mathfrak{p} \in \mathrm{Spec}(A)$, as it is free. Moreover, this rank will be locally constant (in $\mathrm{Spec}(A)$). This tells us that the following definition makes sense.

Definition 3.5. Let P be a finitely generated projective A-module. The *rank* of P is a function $\mathrm{rank}_A(P) : \mathrm{Spec}(A) \to \mathbb{Z}$ defined by $\mathrm{rank}_A(P)(\mathfrak{p}) = n$ if $P_\mathfrak{p} = A_\mathfrak{p}^n$.

The observation we just made tells us that this is a well defined locally constant function, and therefore continuous. In particular, if $\mathrm{Spec}(A)$ is connected, then $\mathrm{rank}_A(P)$ is constant. If the ring A is clear from the context, we may denote just $\mathrm{rank}(P)$ instead of $\mathrm{rank}_A(P)$.

Definition 3.6. Let P be a finitely generated projective A-module. We say that P is *faithfully projective* if $\mathrm{rank}(P) \geq 1$, that is, $\mathrm{rank}(P)(\mathfrak{p}) \geq 1$, $\forall \mathfrak{p} \in \mathrm{Spec}(A)$.

Proposition 3.4. Let A be a ring and P a finitely generated projective A-module. Then, the following statements are equivalent.

i) P is faithfully projective
ii) The map $A \to \mathrm{End}_{\mathbb{Z}}(P)$ that gives the A-module structure is injective
iii) P is faithful, i.e. an A-module $M = 0 \iff M \otimes_A P = 0$
iv) P is faithfully flat, i.e., a sequence of A-modules $M_0 \to M_1 \to M_2$ is exact if and only if $M_0 \otimes P \to M_1 \otimes P \to M_2 \otimes P$ is exact.

Proof. $\boxed{(i) \Rightarrow (iii)}$ Let $M \otimes_A P = 0$. Then, tensoring with $A_{\mathfrak{p}}$ we get $(M \otimes_A P) \otimes_A A_{\mathfrak{p}} \cong M \otimes_A A_{\mathfrak{p}}^n \cong M_{\mathfrak{p}}^n$, with $n \geq 1$ as P is faithfully projective. Then, $M \otimes_A P = 0 \Rightarrow M_{\mathfrak{p}} = 0 \ \forall \mathfrak{p} \in \mathrm{Spec}(A) \Rightarrow M = 0$ by [1], Proposition 3.8.

$\boxed{(iii) \Rightarrow (i)}$ Let $\mathrm{rank}_A(P)(\mathfrak{p}) = 0$, i.e. $P_{\mathfrak{p}} = 0$. Then, $A_{\mathfrak{p}} \otimes P \cong P_{\mathfrak{p}} = 0$, and as P is faithful, this implies that $A_{\mathfrak{p}} = 0$. But this is impossible, so we must have $\mathrm{rank}_A(P) \geq 1$, and so P is faithfully projective.

$\boxed{(iii) \Rightarrow (ii)}$ Let $a \in A$ such that $ax = 0 \ \forall x \in P$. Then, (a) is an ideal of A, and in particular an A-module. This means that $(a) \otimes_A P = 0$, and so we have $(a) = 0$, which implies that $a = 0$ and so the map $A \to \mathrm{End}_{\mathbb{Z}}(P)$ is injective.

$\boxed{(ii) \Rightarrow (i)}$ Suppose that $P_{\mathfrak{p}} = 0$ for a certain prime $P_{\mathfrak{p}}$. Then, as P is finitely generated, let's take $\{x_i\}_{i=1,\dots,n}$ of generators of P. We know that $\exists f_1, \dots, f_n \notin \mathfrak{p}$ such that $x_i f_i = 0$, and we must have $f_1 \dots f_n \notin \mathfrak{p}$, because $\mathfrak{p}$ is prime. Then, we have $(f_1 \dots f_n)x = 0 \forall x \in P$. This contradicts (ii), as $f_1 \dots f_n \neq 0$.

$\boxed{(iv) \Rightarrow (iii)}$ Take the sequence $0 \to M \to 0$.

$\boxed{(iii) \Rightarrow (iv)}$ We already know that every projective module is flat. Therefore we just need to prove the reverse implication. Consider the sequence $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$, and let $M_0 \otimes P \xrightarrow{f \otimes \mathrm{id}_P} M_1 \otimes P \xrightarrow{g \otimes \mathrm{id}_P} M_2 \otimes P$ be exact. Note that $\ker(g) \supseteq \mathrm{im}(f)$, as $0 = (g \otimes \mathrm{id}_P) \circ (f \otimes \mathrm{id}_P)(M_0 \otimes P) = g(f(M_0)) \otimes P$, and by (iii) this implies that $g(f(M_0)) = 0 \Rightarrow \mathrm{im}(f) \subseteq \ker(g)$

Then, there is a well defined map $\overline{g} : M_1/f(M_0) \to M_2$, such that the induced map $\overline{g} \otimes \mathrm{id}_P : M_1/f(M_0) \otimes P \to M_2 \otimes P$ is injective. Then, suppose that we have $x \in M_1, x \notin f(M_0)$ such that $g(x) = 0$. Consider $\overline{x}$ the image of x in $M_1/f(M_0)$. $\overline{g}(A\overline{x}) \otimes P = 0$, which implies $A\overline{x} \otimes P = 0$ by injectivity of the map $\overline{g} \otimes P$. Finally, by (iii) this implies that $A\overline{x} = 0 \Rightarrow x \in f(M_0)$. In conclusion, $\mathrm{im}(f) \supseteq \ker(g)$. □

3.3 Projective algebras

Given a ring A and an A-algebra B, we can regard B as an A-module. This way we can apply all the concepts of projective modules to algebras.

Definition 3.7. Let A be a ring and B an A-algebra. We say that B is a *projective algebra* if it is projective as an A-module, and that B is *finite projective* if it is finitely generated projective as an A-module.

For a finite projective algebra, we denote by $[B : A] := \mathrm{rank}_A(B)$. We say that B is *faithfully projective* if it is faithfully projective as a module.

Proposition 3.5. Let B be a finite projective A-algebra. Then we have

i) The map $A \to B$ is injective $\iff$ B is faithfully projective.
ii) The map $A \to B$ is surjective if and only if $[B : A] \leq 1$, and if and only if the map $B \otimes_A B \to B$, $x \otimes y \mapsto xy$ is an isomorphism.

iii) The map $A \to B$ is an isomorphism if and only if $[B : A] = 1$.

Proof. This proof relies basically on [1], Proposition 3.9, which states that an A-module homomorphism ϕ is injective/surjective/an isomorphism if and only if $\forall \mathfrak{p} \in \mathrm{Spec}(A)$, $\phi_{\mathfrak{p}}$ is injective/surjective/an isomorphism.

i) Suppose that $[B : A](\mathfrak{p}) = 0$. Then $B_{\mathfrak{p}} = 0$, so $A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ is not injective, and therefore $A \to B$ is not injective. Reciprocally, let $[B : A] \geq 1$. The kernel of the map $A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ anihilates $B_{\mathfrak{p}}$, but as $B_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$ module, then $\ker(A_{\mathfrak{p}} \to B_{\mathfrak{p}}) = 0$ and the map $A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ is injective. As this holds $\forall \mathfrak{p}$, then the map $A \to B$ is also injective.

ii) First suppose that the map $B \otimes_A B \to B$ is an isomorphism. Localizing in $A_{\mathfrak{p}}$, it is immediate that $B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{p}} \cong A_{\mathfrak{p}}^{n^2}$, if $B_{\mathfrak{p}} \cong A_{\mathfrak{p}}^n$ as $A_{\mathfrak{p}}$-modules. Then, as we know that two free modules are isomorphic if and only if they have the same rank (Proposition A.2), we must have $[B : A]^2 = [B : A]$, and so $[B : A] \leq 1$.

Now let $[B : A] \leq 1$. As it is enough to prove the surjectivity for $A_{\mathfrak{p}} \to B_{\mathfrak{p}}$, we can assume that A is local and so B is free and the rank is constant. Let's analyze the two cases separately.

- $[B : A] = 0$. This implies $B = 0$, and so the map is surjective.
- $[B : A] = 1$. B is free of rank 1 over A, and so also $\mathrm{End}_A(B)$ is free of rank 1 over A, and the identity map forms a basis. Then, we have the injective map $\psi : B \to \mathrm{End}_A(B)$, $b \mapsto m_b$ multiplication by b. The composition $A \to B \to \mathrm{End}_A(B)$ yields an isomorphism, as it maps a basis of A (1) to a basis of $\mathrm{End}_A(B)$ (the identity). Therefore, $A \to B$ must be surjective.

Finally, if $A \to B$ is surjective, we have $B \cong A/\mathfrak{a}$, for a certain ideal of A that anihilates B. So $B \otimes_A B \cong B/\mathfrak{a}B$, and as $\mathfrak{a}B = 0$, $B/\mathfrak{a}B = B$. The composition of these isomorphisms yields exactly the map $B \otimes B \to B$ mapping $x \otimes y \mapsto xy$.

iii) Is an immediate consequence of (i) and (ii).

□

Lemma 3.5. Let A be a ring, B an A-algebra and P a projective A-module. Then $P \otimes_A B$ is a projective B-module, and the diagram

$$\begin{tikzcd}
\mathrm{Spec}(B) \arrow[r] \arrow[d, "\mathrm{rank}_B(P\otimes_A B)"'] & \mathrm{Spec}(A) \arrow[dl, "\mathrm{rank}_A(P)"] \\
\mathbb{Z} &
\end{tikzcd}$$

commutes if P is finitely generated.

Proof. If P is projective and finitely generated, there exists a finitely generated module Q such that $P \oplus Q \cong A^n$. Therefore, $(P \otimes_A B) \oplus (Q \otimes_A B) \cong B^n$ as B-modules, and so $P \otimes_A B$ is a projective B-module. Now let $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{p} = \mathfrak{q}^c$. Then, the induced map $A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ induces the natural $A_{\mathfrak{p}}$-module structure on $B_{\mathfrak{q}}$.

We just need to check that $(P \otimes_A B) \otimes_B B_{\mathfrak{q}}$ and $P \otimes_A A_{\mathfrak{p}}$ have the same rank. If we denote $n = \mathrm{rank}_{A_{\mathfrak{p}}}(P_{\mathfrak{p}})$, as $P_{\mathfrak{p}} = P \otimes_A A_{\mathfrak{p}}$, we have then that $P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}} \cong B_{\mathfrak{q}}^n$ as $B_{\mathfrak{q}}$-modules. We know that 2 free modules are isomorphic if and only if they have the same rank (Proposition A.2), and therefore it will be enough to prove that $(P \otimes_A B) \otimes_B B_{\mathfrak{q}}$ is isomorphic to $P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}}$ as $B_{\mathfrak{q}}$-modules. First note that $(P \otimes_A B) \otimes_B B_{\mathfrak{q}} \cong P \otimes_A B_{\mathfrak{q}}$. So we have to prove $P \otimes_A B_{\mathfrak{q}} \cong P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}}$.

Now consider the map $P \times B_{\mathfrak{q}} \to P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}}$ defined by $(p, \frac{b}{t}) \mapsto \frac{p}{1} \otimes \frac{b}{t}$. This is a well-defined A-bilinear map, and therefore it induces a map $P \otimes_A B_{\mathfrak{q}} \to P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}}$. Reciprocally, the map $P_{\mathfrak{p}} \times B_{\mathfrak{q}} \to P \otimes_A B_{\mathfrak{q}}$ defined by $(\frac{p}{s}, \frac{b}{t}) \mapsto (p \otimes \frac{b}{ts})$ is $A_{\mathfrak{p}}$-bilinear.

Let's check that it is well defined. On the first coordinate, let $\frac{p}{s} = \frac{p'}{s'} \Rightarrow \exists u \notin \mathfrak{p}$ such that $(s'p - p's)u = 0$. Then, $p \otimes \frac{b}{ts} = p \otimes \frac{bus'}{tsus'} = pus' \otimes \frac{b}{tsus'} = pus \otimes \frac{b}{tsus'} = p'us \otimes \frac{b}{tsus'} = p' \otimes \frac{b}{ts'}$. The argument is immediate for the second coordinate. It's clear that the two maps $P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}} \leftrightarrow P \otimes_A B_{\mathfrak{q}}$ are inverses, and so $P_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{q}} \cong P \otimes_A B_{\mathfrak{q}}$ and we are done. □

Proposition 3.6. Let B be a faithfully flat A-algebra, 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. The direct implication is true even if we remove the faithfully flat condition for B, by the lemma above. Let's see the other implication. Let $\{p_i \otimes 1\}_{i=1}^{n}$ be a finite set of generators of $P \otimes_A B$. Then, we have a natural A-linear map $A^n \to P$ that maps the $i - th$ basic element of A^n to $p_i \otimes 1$. This map is surjective when we tensor it with B. But as B is faithfully flat, then $A^n \to P$ is also surjective, and this proves that P is also finitely generated.

Then, we have an exact sequence $0 \to Q \to A^n \to P \to 0$. Tensoring with B we obtain $0 \to Q \otimes B \to B^n \to P \otimes B \to 0$, exact sequence (as B is flat). Then, the sequence splits, as $P \otimes B$ is a projective B-module. $Q \otimes B$ is therefore a direct summand of B^n and so $Q \otimes B$ is projective and finitely generated. Using the same argument that we just made with P, we conclude that Q is finitely generated, and so P is finitely presented.

Now let M be any A-module. Consider the map

$$\begin{aligned} \mathrm{Hom}_A(P, M) \otimes_A B &\longrightarrow \mathrm{Hom}_B(P \otimes_A B, M \otimes_A B) \\ f \otimes b &\longmapsto \qquad f' : P \otimes_A B \longrightarrow M \otimes_A B \\ &\qquad\qquad\qquad p \otimes b' \longmapsto f(p) \otimes bb' \end{aligned}$$

We will now prove that, if P is finitely presented (which is our case) this map is an isomorphism of B-modules.

In the case where $P = A^n$, we have $\mathrm{Hom}_A(A^n, M) \cong M^n \Rightarrow \mathrm{Hom}_A(A^n, M) \otimes B \cong (M \otimes B)^n$ and $\mathrm{Hom}_B(A^n \otimes B, M \otimes B) \cong (M \otimes B)^n$, as every homomorphism is totally defined by the image of the basis elements. Then, the map defined and these isomorphisms yield a commutative diagram

$$\begin{tikzcd} \mathrm{Hom}_A(A^n, M) \otimes_A B \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_B(P \otimes_A B, M \otimes_A B) \arrow[d, "\cong"] \\ (M \otimes B)^n \arrow[r, "\mathrm{id}"] & (M \otimes_A B)^n \end{tikzcd}$$

which proves our statement for $P = A^n$. In the general case P is finitely presented, so we have an exact sequence $A^m \to A^n \to P \to 0$. Using the flatness of B and the right-exactness of $\mathrm{Hom}_A(-, M)$ we have the following commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_A(P, M) \otimes_A B \arrow[r] \arrow[d, "3"] & \mathrm{Hom}_A(A^n, M) \otimes_A B \arrow[r] \arrow[d, "1"] & \mathrm{Hom}_A(A^m, M) \otimes_A B \arrow[d, "2"] \\ 0 \arrow[r] & \mathrm{Hom}_B(P \otimes_A B, M \otimes_A B) \arrow[r] & \mathrm{Hom}_B(A^n \otimes_A B, M \otimes_A B) \arrow[r] & \mathrm{Hom}_B(A^m \otimes_A B, M \otimes_A B) \end{tikzcd}$$

As $1, 2$ are isomorphisms, then 3 must also be an isomorphism. In conclusion the map $\mathrm{Hom}_A(P, M) \otimes_A B \to \mathrm{Hom}_B(P \otimes_A B, M \otimes_A B)$ is an isomorphism.

To end the proof, suppose that we have 2 A-modules, M and N, and a surjective morphism $M \to N$. As B is flat, then the map $M \otimes_A B \to N \otimes_A B$ is surjective. As $P \otimes_A B$ is projective, the map $\mathrm{Hom}_B(P \otimes_A B, M \otimes_A B) \to \mathrm{Hom}_B(P \otimes_A B, N \otimes_A B)$ is also surjective. Now, making use of the isomorphism we have just found, we know that also the map $\mathrm{Hom}_A(P, M) \otimes_A B \to \mathrm{Hom}_A(P, N) \otimes_A B$ is surjective. Finally, using that B is faithfully flat, we conclude that the map $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N)$ is surjective. So we have proved the characterization of Proposition 3.1 (ii), and therefore P is projective over A. □

Lemma 3.6. Let A be a ring, and B a finite projective A-algebra. Let P be a finitely generated projective B-module. Then P is a finitely generated projective A-module when regarded by restriction of scalars.

Proof. Let $x_1, \dots, x_k \in B$ be generators of B as an A-module, and let $y_1, \dots, y_r$ be generators of P as a B-module. Then, the set $\{x_i y_j\}_{i,j}$ generates P as an A-module, so P is finitely generated.

In addition, as B is a finitely generated projective A-module, exists Q such that $B \oplus Q \cong A^m$. Similarly, there exists a B-module Q' such that $P \oplus Q' \cong B^n$ as B-modules. By restriction of scalars, $P \oplus Q' \cong B^n$ is also an isomorphism of A-modules. Then, $P \oplus Q' \oplus Q^n \cong B^n \oplus Q^n \cong (B \oplus Q)^n \cong A^{nm}$ as A-modules. Therefore, P is a direct summand of a free A-module, and so it is projective. □

3.4 Projective separable algebras

In the Introduction, we gave the definition of a free separable algebra. Now we will extend the notion of separability to the case of projective algebras. To do that, we need to find a definition of trace that works for projective modules. Given an A-module M we will denote its dual by $M^* = \mathrm{Hom}_A(M, A)$.

Lemma 3.7. Let P be a finitely generated projective A-module, and let M be any A-module. Then, the map

$$\begin{aligned} \phi : P^* \otimes_A M &\longrightarrow \mathrm{Hom}_A(P, M) \\ f \otimes m &\longmapsto \phi(f \otimes m) : P \longrightarrow M \\ &\qquad\qquad\qquad\qquad p \longmapsto f(p)m \end{aligned}$$

is an isomorphism of A-modules. When there is a possible confusion on the modules involved, we will denote the map as $\phi_{P,M}$.

Proof. Let first $P = A$. Every A-linear map $f : A \to M$ is totally determined by $f(1)$, as then $f(a) = af(1) \in M$. Reciprocally, every choice of an element of $m \in M$ defines an A-linear map $f_m : A \to M$ by setting $f(1) = m$ and extending by linearity. Therefore, $\mathrm{Hom}_A(A, M) \cong M$ via the isomorphism $f \mapsto f(1)$. Moreover, the map $M \to A \otimes M$ defined by $m \mapsto 1 \otimes m$ is an isomorphism (the map induced by the A-bilinear map $A \times M \to M$, $(a, m) \mapsto am$ is its inverse).

Then, the composition of the maps $M \cong A \otimes M \cong A^* \otimes M \xrightarrow{\phi_{A,M}} \mathrm{Hom}_A(A, M) \cong M$ yields the identity, and this proves that the map $\phi_{A,M}$ is an isomorphism, so the case with $P = A$ holds. Using the natural isomorphism $\mathrm{Hom}_A(\bigoplus_{i=1}^n A, N) \cong \bigoplus_{i=1}^n \mathrm{Hom}_A(A, N)$, we have the chain of isomorphisms

$$\mathrm{Hom}_A(A^n, N) \otimes M \cong \bigoplus_{i=1}^n \mathrm{Hom}_A(A, N) \otimes M \xrightarrow[\cong]{\phi_{A,M}} \bigoplus_{i=1}^n \mathrm{Hom}_A(A, M) \cong \mathrm{Hom}_A(A^n, M)$$

that yields $\phi_{A^n,M}$, and so the statement also holds for free modules. Finally, let P be a finitely generated projective module. Then $\exists Q$ finitely generated such that $P \oplus Q \cong A^n$, and we have

$$(P^* \otimes M) \oplus (Q^* \otimes M) \cong \mathrm{Hom}_A(A^n, A) \otimes M \xrightarrow[\cong]{\phi_{A,M}} \mathrm{Hom}_A(A^n, M) \cong \mathrm{Hom}_A(P, M) \oplus \mathrm{Hom}_A(Q, M)$$

This isomorphism corresponds on the first coordinate to $\phi_{P,M}$, and so using that a sum of exact sequences is exact if and only if each sequence is exact, we conclude that $\phi_{P,M}$ is an isomorphism. □

Definition 3.8. Let P be a finitely generated projective A-module. Then, we define the *trace of P over A* as the A-linear map $Tr = Tr_{P/A} : \mathrm{End}_A(P) \to A$ defined as the composition of $\phi_{P,P}^{-1}$ with the natural map $P^* \otimes_A P \to A$, $f \otimes p \mapsto f(p)$.

$$Tr_{P/A} : \mathrm{End}_A(P) \xrightarrow{\phi_{P,P}^{-1}} P^* \otimes_A P \to A$$

Note that the previous lemma tells us that this definition makes sense, as $\phi_{P,P}$ is an isomorphism and so we can talk about its inverse $\phi_{P,P}^{-1}$.

Definition 3.9. Let A be a ring, B a finite projective A-algebra. We say that B is *projective separable* if the A-linear map

$$\begin{aligned} \varphi : B &\longrightarrow \mathrm{Hom}_A(B, A) \\ b &\longmapsto \quad \varphi(b) : B \longrightarrow A \\ &\qquad\qquad x \longmapsto (\varphi(b))(x) = \mathrm{Tr}(bx) \end{aligned}$$

is an isomorphism of A-modules. When there is confusion on the rings and modules involved, we will denote $\varphi_{B/A}$.

Observation 3.4. The definition of separability that we have just given is the same that we gave in the Introduction, but where we have changed the definition of the trace. Therefore, to regard this definition as an extension of the free module case to the projective case, we just have to check that the definition of trace just given agrees with the usual one if P is a free module.

Let $\{w_i\}_{i=1}^n$ be a basis of P. Note that P^* is free, and we can take as a basis $\{w_i^*\}$, where $w_i^*(w_j) = \delta_{ij}$ is the usual dual basis. Now take $f \in \mathrm{End}(P)$, defined by $f(w_i) = \sum_{i=1}^n a_{ij} w_j$. Note that $\phi(\sum_{i,j} a_{ij} w_i^* \otimes w_j)(w_k) = \sum_j a_{kj} w_j$, and so $\phi^{-1}(f) = \sum_{i,j} a_{ij} w_i^* \otimes w_j$. Therefore, $Tr(f) = \sum_{ij} a_{ij} w_i^*(w_j) = \sum_i a_{ii}$, which agrees with the usual definition of the trace for free modules.

Observation 3.5. The terminology used may usually lead to confusion, because we speak of "free separable algebras" and "projective separable algebras". In fact, there exists a general definition of a separable algebra that doesn't require the algebra to be free or projective, and it can be seen that the definitions that have been given are equivalent to "free and separable" and "projective and separable", respectively (see [5], 6.10). By the observation above, in our situation we can speak of "separable algebras" without having to bother about which definition ("projective separable" or "free separable") are we using. However, we always have to require our algebra to be atleast projective. Moreover, it should also be noted that, in our situation, when we speak of "free separable" or "projective separable" algebras, we always implicitely mean that these algebras have to be finite.

Let's now prove some basic properties of projective separable algebras.

Lemma 3.8. Let A be a ring, B an A-algebra, P a finitely generated projective A-module. Then, the following diagram is commutative

$$\begin{tikzcd}
\mathrm{End}_A(P) \arrow[r, "\otimes \mathrm{id}_B"] \arrow[d, "Tr_{P/A}"] & \mathrm{End}_B(P \otimes_A B) \arrow[d, "Tr_{P\otimes_A B/B}"] \\
A \arrow[r] & B
\end{tikzcd}$$

Proof. Let $f \otimes p \in P^* \otimes_A P$, and consider $f' = f \otimes \mathrm{id}_B : P \otimes_A B \to B$, that is, $f'(p \otimes b) = f(p)b$. Let's define the map $\psi : P^* \otimes_A P \to (P \otimes_A B)^* \otimes_B (P \otimes_A B)$ by $f \otimes p \mapsto (f \otimes \mathrm{id}_B) \otimes (p \otimes 1)$. Now, consider the following diagram:

$$\begin{tikzcd}
\mathrm{End}_A(P) \arrow[d, "-\otimes \mathrm{id}_B"] & P^* \otimes_A P \arrow[l, "\phi_{P,P}"'] \arrow[d, "\psi"] \\
\mathrm{End}_B(P \otimes_A B) & (P \otimes_A B)^* \otimes_B (P \otimes_A B) \arrow[l, "\phi_{P\otimes_A B, P\otimes_A B}"']
\end{tikzcd}$$

Given $f \otimes p \in P^* \otimes P$, $\phi_{P,P}$ sends it to the map $\phi_{P,P}(f \otimes p) : x \mapsto f(x)p$. Therefore, $\phi_{P,P}(f \otimes p) \otimes \mathrm{id}_B : x \otimes b \mapsto f(x)p \otimes b$. On the other side, $\psi(f \otimes p) = (f \otimes \mathrm{id}_B) \otimes (p \otimes 1)$, and so $\phi_{P \otimes_A B}(\psi(f \otimes p)) : x \otimes b \mapsto f(x)b(p \otimes 1) = f(x)p \otimes b$. This proves that the diagram is commutative, and then it is immediate that the diagram with the horizontal arrows reversed is also commutative.

In addition, let's consider the diagram

$$\begin{tikzcd}
P^* \otimes_A P \arrow[r, "\psi"] \arrow[d] & (P \otimes_A B)^* \otimes_B (P \otimes_A B) \arrow[d] \\
A \arrow[r] & B
\end{tikzcd}$$

with evaluation maps as vertical arrows. This diagram is also commutative. Indeed, take $f \otimes p \in P^* \otimes_A P$. Then, $\psi(f \otimes p) = (f \otimes \mathrm{id}_B) \otimes (p \otimes 1)$, and when we evaluate it, it yields $f(p)1 \in B$.

Putting all together, we see that the full diagram of the statement is commutative

$$\begin{tikzcd}
\mathrm{End}_A(P) \arrow[r, "-\otimes \mathrm{id}_B"] \arrow[d, "\phi_{P,P}^{-1}"] \arrow[dd, bend right=60, "Tr_{P/A}"'] & \mathrm{End}_B(P \otimes_A B) \arrow[d, "\phi^{-1}_{P\otimes_A B, P\otimes_A B}"] \arrow[dd, bend left=60, "Tr_{P\otimes_A B/B}"] \\
P^* \otimes_A P \arrow[r, "\psi"] \arrow[d] & (P \otimes_A B)^* \otimes_B (P \otimes_A B) \arrow[d] \\
A \arrow[r] & B
\end{tikzcd}$$

□

Lemma 3.9. Let $0 \to P_0 \to P_1 \to P_2 \to 0$ be an exact sequence of A-modules, with P_1, P_2 finitely generated and projective. Let $g : P_1 \to P_1$ be an A-linear map, with $g(P_0) \subseteq P_0$, and let $h : P_2 \to P_2$ be the map induced by g. Then, P_0 is finitely generated and projective, and $Tr_{P_1/A}(g) = Tr_{P_0/A}(g|_{P_0}) + Tr_{P_2/A}(h)$.

Proof. Given an exact sequence $M_0 \to M_1 \to M_2$, we have that the induced sequence $\mathrm{Hom}_A(P_1, M_0) \to \mathrm{Hom}_A(P_1, M_1) \to \mathrm{Hom}_A(P_1, M_2)$ is exact, as P_1 is projective. As P_2 is projective, the sequence $0 \to P_0 \to P_1 \to P_2 \to 0$ splits, so we have $P_1 \cong P_0 \oplus P_2$, and therefore $\mathrm{Hom}_A(P_1, N) \cong \mathrm{Hom}_A(P_0, N) \oplus \mathrm{Hom}_A(P_2, N)$. So we have the exact sequence

$$\mathrm{Hom}_A(P_0, M_0) \oplus \mathrm{Hom}_A(P_2, M_0) \to \mathrm{Hom}_A(P_0, M_1) \oplus \mathrm{Hom}_A(P_2, M_1) \to \mathrm{Hom}_A(P_0, M_2) \oplus \mathrm{Hom}_A(P_2, M_2)$$

This implies that the sequences when we restrict to each coordinate are exact, and so looking at the first coordinate we obtain that P_0 is projective. The fact that $P_1 \cong P_0 \oplus P_2$ implies that P_0 is also finitely generated.

It is immediate that, under the isomorphism $P_0 \oplus P_2 \cong P_1$, the endomorphism g corresponds to the pair of maps $(g|_{P_0}, h)$. Taking into account the expression of the isomorphism $P_0 \oplus P_2 \cong P_1$, and the induced isomorphism on dual spaces, it is also clear that the following diagram is commutative.

$$\begin{tikzcd}
P_1^* \otimes P_1 \arrow[r] \arrow[d] & A \arrow[d] \\
(P_0 \oplus P_2)^* \otimes (P_0 \oplus P_2) \arrow[r] & A
\end{tikzcd}$$

On the other side, let's consider the diagram

$$\begin{tikzcd}
P_1^* \otimes P_1 \arrow[r, "\phi_{P_1, P_1}"] \arrow[d] & \mathrm{End}(P_1) \arrow[d] \\
(P_0 \oplus P_2)^* \otimes P_0 \oplus P_2 \arrow[r, "\phi_{P_0 \oplus P_2, P_0 \oplus P_2}"] & \mathrm{End}(P_0 \oplus P_2)
\end{tikzcd}$$

Consider an element $f \otimes p \in P_1^* \otimes P_1$, and let $(f_0, f_2) \otimes (p_0, p_2)$ be the corresponding element in $(P_0 \oplus P_2)^* \otimes (P_0 \oplus P_2)$. Both paths of the diagram send the element $f \otimes p$ to a map $\alpha : P_0 \oplus P_2 \to P_0 \oplus P_2$ defined by $(x_0, x_2) \mapsto (f_0(x_0) + f_2(x_2))(p_1, p_2)$, and so the diagram is commutative.

The diagram will remain commutative if we reverse the horizontal arrows (recall that they're isomorphisms). Putting everything together, we have the following commuative diagram

$$\begin{tikzcd}
\mathrm{Hom}_A(P_1, P_1) \arrow[r, "\phi_{P_1}^{-1}"] \arrow[d] \arrow[rr, bend left, "Tr_{P_1/A}"] & P_1^* \otimes P_1 \arrow[r] \arrow[d] & A \arrow[d] \\
\mathrm{Hom}_A(P_0 \oplus P_2, P_0 \oplus P_2) \arrow[r, "\phi_{P_0 \oplus P_2}^{-1}"] \arrow[rr, bend right, "Tr_{(P_0 \oplus P_2)/A}"'] & (P_0 \oplus P_2)^* \otimes (P_0 \oplus P_2) \arrow[r] & A
\end{tikzcd}$$

□

Proposition 3.7. Let B be an A-algebra, C a faithfully flat A-algebra such that $B \otimes_A C$ is a projective separable C-algebra. Then B is a projective separable A-algebra.

Proof. We already know that B is finite projective, by Proposition 3.6. We just need to check that the map $\varphi_{B/A} : B \to \mathrm{Hom}_A(B, A)$ of the definition of separability is an isomorphism. As C is faithfully projective, it is faithfully flat (Proposition 3.4), and therefore it will be enough to show that the map $\varphi_{B/A} \otimes \mathrm{id}_C : B \otimes_A C \to \mathrm{Hom}_A(B, A) \otimes_A C$ is an isomorphism. Consider the map

$$B \otimes_A C \xrightarrow{\varphi_{B/A} \otimes \mathrm{id}_C} \mathrm{Hom}_A(B, A) \otimes_A C \xrightarrow{\cong} \mathrm{Hom}_C(B \otimes_A C, C) \tag{1}$$

Where the second map is the same as in the proof of Proposition 3.6, composed with the usual isomorphism $C \otimes_A A \cong C$. It is an isomorphism because we already know that B is finite projective.

Let's see how this acts on an element of the form $b \otimes c$. The first map sends it to $\varphi_{B/A}(b) \otimes c$, and the image of $\varphi_{B/A}(b) \otimes c$ via the second map is a morphism $\alpha : B \otimes_A C \to C$, defined by $b' \otimes c' \mapsto \varphi_{B/A}(b)(b')cc' = Tr_{B/A}(bb')cc'$.

On the other hand, the map $\varphi_{B \otimes_A C/C} : B \otimes_A C \to \mathrm{Hom}_C(B \otimes_A C, C)$ maps an element $b \otimes c$ to a map $b' \otimes c' \mapsto Tr_{B \otimes_A C/C}(bb' \otimes cc')$. By C-linearity, $Tr_{B \otimes_A C/C}(bb' \otimes cc') = Tr_{B \otimes_A C/C}(bb' \otimes 1)cc'$. Now, using Lemma 3.8, $Tr_{B \otimes_A C/C}(bb' \otimes 1)cc' = Tr_{B/A}(bb')cc'$. Therefore, the map in 1 is exactly the morphism $\varphi_{B \otimes_A C/C}$, and therefore, it is an isomorphism as $B \otimes_A C$ is projective separable. This implies that also $\varphi_{B/A} \otimes \mathrm{id}_C$ is an isomorphism, and we are done. □

From the proof of this proposition, it is immediate that the reciprocal also holds:

Proposition 3.8. Let B be a projective separable A-algebra, and C any A-algebra. Then, $B \otimes_A C$ is a projective separable C-algebra.

Proof. If $\varphi_{B/A} : B \to \mathrm{Hom}_A(B, A)$ is an isomorphism, then tensoring preserves this isomorphism, so $B \otimes_A C \to \mathrm{Hom}_A(B, A) \otimes C$ is an isomorphism. Therefore the map in 1 is an isomorphism, and we know from the proof of last proposition that it is the map $\varphi_{B \otimes C/C}$. In conclusion, $\varphi_{B \otimes C/C}$ is an isomorphism of C-modules, and so $B \otimes_A C$ is a projective separable C-algebra. □

This result tells us that base changes preserve the property of being projective separable. The following tells us that products of projective separable algebras are also projective separable.

Lemma 3.10. Let $B_1, \dots, B_n$ projective separable algebras over a ring A. Prove that $\prod_{i=1}^n B_i$ is a projective separable A-algebra if and only if each B_i is a projective separable A-algebra.

Proof. Let $M_0 \to M_1 \to M_2$ be an exact sequence of A-modules. Taking into account that $\forall$ A-module N we have an isomorphism $\mathrm{Hom}_A(\prod_{i=1}^n B_i, N) \cong \bigoplus_{i=1}^n \mathrm{Hom}_A(B_i, N)$, then the sequence $\mathrm{Hom}_A(\prod_{i=1}^n B_i, M_0) \to \mathrm{Hom}_A(\prod_{i=1}^n B_i, M_1) \to \mathrm{Hom}_A(\prod_{i=1}^n B_i, M_2)$ will be exact if and only if the sequence

$$\bigoplus_{i=1}^n \mathrm{Hom}_A(B_i, M_0) \to \bigoplus_{i=1}^n \mathrm{Hom}_A(B_i, M_1) \to \bigoplus_{i=1}^n \mathrm{Hom}_A(B_i, M_2)$$

is exact. At its turn, this happens if and only if the sequence is exact on each coordinate. In conclusion, $\prod_{i=1}^n B_i$ is projective if and only if each B_i is projective.

Applying the same arguent on the map $\varphi_{\prod_{i=1}^n B_i/A} : \prod_{i=1}^n B_i \to \mathrm{Hom}_A(\prod_{i=1}^n B_i, A)$ we see that this is an isomorphism if and only if each of the maps $\varphi_{B_i/A} : B_i \to \mathrm{Hom}_A(B_i, A)$ is an isomorphism. In conclusion, $\prod_{i=1}^n B_i$ is projective separable if and only if each B_i is projective separable. □

Theorem 3.2. *i) Let B' be a projective separable A-algebra, and $f : B' \to A$ an A-algebra homomorphism. Then, $\exists$ an A-algebra C and $B' \cong A \times C$ isomorphism of A-algebras such that f is the composition of $B' \to A \times C$ and the projection $A \times C \to A$.*

ii) Let A be a ring, and B a projective separable A-algebra. Consider the B-algebra $B \otimes_A B$ via the second factor. Then, there exists a B-algebra C and an isomorphism $B \otimes_A B \xrightarrow{\cong} B \times C$ such that the composition with the projection $B \times C \to B$ yields the map $B \otimes_A B \to B$, $x \otimes y \mapsto xy$.

Proof. i) As B' is projective separable, $\exists e \in B'$ such that $f(x) = Tr_{B'/A}(ex)$, $\forall x \in B'$. Taking into account that f is an A-algebra morphism, and setting $x = 1$, we obtain $Tr_{B'/A}(e) = f(1) = 1$. Moreover, we have $Tr_{B'/A}(exy) = f(xy) = f(x)f(y) = f(x)Tr_{B'/A}(ey) = Tr_{B'/A}(f(x)ey)$. Using the separability again, we must have $ex = f(x)e$, $\forall x \in B'$. In particular, if we take $x \in \ker f$, this yields $ex = 0$, and so $e \ker f = 0$. On the other side, we have the exact sequence $0 \to \ker f \to B' \xrightarrow{f} A \to 0$. Then, using Lemma 3.9, we have that $1 = Tr_{B'/A}(e) = Tr_{\ker f/A}(e|_{\ker f}) + Tr_{A/A}(f(e)) = f(e)$, and so $f(e) = 1$.

Consider the map $A \to B'$, $1 \mapsto e$. As the composition with f yields the identity, then the exact sequence $0 \to \ker f \to B' \to A \to 0$ splits, so it induces an isomorphism $h : A \oplus \ker f \cong B'$, $(a, b) \mapsto ae + b$. Now, taking $x = e$ in the identity $ef(x) = ex$, we get $e^2 = e$, and combining this with the fact that $e \ker f = 0$, we have $(a_1 e + b_1)(a_2 e + b_2) = a_1 a_2 e + b_1 b_2$.

Finally, as A, B' have units, $\ker f$ must also have a unit, and therefore $C = \ker f$ is the A-algebra we were looking for: $A \times C \cong A \oplus C = A \oplus \ker f \cong B'$. This proves that the map h is in fact an isomorphism of A-algebras, and not just of A-modules.

Note that an element $(a, b) \in A \times C$ corresponds via h to $ae + b \in B'$. $f(ae + b) = a$, which agrees with the projection on the first coordinate of (a, b).

ii) We know that $B \otimes_A B$ is a projective separable B-algebra by Proposition 3.8. The map $f : B \otimes_A B \to B$ defined by $f(x \otimes y) = xy$ is a B-algebra homomorphism. Now the result easily follows from applying (i), taking A to be B, B' to be $B \otimes_A B$ and the B-algebra homomorphism f.

□

By now we have introduced the notion of projective separable algebra and given some properties, but we haven't already seen any example of projective separable algebras, appart from the case of free separable algebras over fields that we dealt with in Lemma 2.1.

Example 3.2. Let A be a ring, and $f \in A[x]$ a monic polynomial, $f = x^n + a_1 x^{n-1} + \cdots + a_n$ such that $(f', f) = (1)$. Then, $B = A[x]/(f)$ is a finite projective separable algebra.

We will need to make some remarks before proving it. First, let B be any A-algebra, and consider the A-module $B^* = \mathrm{Hom}_A(B, A)$. We will proceed to define a structure of B-module on B^* as follows

$$B \times B^* \to B^*$$
$$(b, f) \mapsto bf : x \mapsto f(bx)$$

This is indeed a well defined B-module structure:

- $b(f + g)(x) = (f + g)(bx) = f(bx) + g(bx) = (bf + bg)(x)$ so $b(f + g) = bf + bg$.
- $(b + b')f(x) = f((b + b')x) = f(bx) + f(b'x) = bf(x) + b'f(x)$, and so $(b + b')f = bf + b'f$

- $1f(x) = f(x) \Rightarrow 1f = f$

Now suppose that B is a free A-module. With the B-module structure just defined, we claim that the trace map on B, $Tr_{B/A} : B \mapsto A$, $b \mapsto Tr(b)$ can be written as $Tr_{B/A} = \sum_{i=1}^{n} e_i e_i^*$, where $\{e_i\}_{i=1}^{n}$ is a basis of B and $\{e_i^*\}_{i=1}^{n}$ is the associated dual basis.

Indeed, let $be_i = \sum_{j=1}^{n} a_{ij} e_j$. Then the trace of b is defined as $Tr(b) = \sum_{i=1}^{n} a_{ii}$. On the other hand, $\sum_{i=1}^{n} e_i e_i^*(b) = \sum_{i=1}^{n} e_i^*(be_i) = \sum_{i=1}^{n} e_i^*(\sum_{j=1}^{n} a_{ij} e_j) = \sum_{i=1}^{n} a_{ii}$. So we have proven that

$$Tr_{B/A} = \sum_{i=1}^{n} e_i e_i^*$$

Now let's move to the proof of the example that we are interested in.

Proof. First let's prove that $B = A[x]/(f)$, where f is a monic polynomial with coefficients in A, is a finitely generated and free A-module. It is obvious that the set $\{1, x, x^2, \dots, x^{n-1}\}$ generates B as an A-module. Let's check that, in addition, it is a basis of B. Let $g(x) = \sum_{i=0}^{n-1} c_i x^i = 0 \in B$, with $a_i \in A$. This implies that $g = fh \in A[x]$. Let α be the coefficient of highest degree of h, ie $h = \alpha x^k + \dots$. Then, αx^{n+k} is the term of highest degree of g, but as g has degree $n-1$, this implies that $\alpha = 0$. We conclude that $h(x) = 0$, and so $g(x) = 0 \in A[x]$, which means that $c_i = 0 \forall i$, and so we conclude that $\{1, x, x^2, \dots, x^{n-1}\}$ is a basis of B. Note that we used here that f is a monic polynomial, otherwise this proof doesn't work.

Now let's consider the ring $B[X]$. To avoid confusions, we will denote as z the class of $x \in B = A[x]/(f)$ from now on. Consider $f(X) = X^n + a_1 X^{n-1} + \dots + a_n$ as a polynomial in $B[X]$, and note that f has a root in B, as $f(z) = 0 \in B$, so $f(X) = (X - z)g(X)$, where $g(X) = \sum_{i=0}^{n-1} b_i X^i$ is a polynomial in $B[X]$, that is, $b_i \in B$.

Deriving at both sides of the expression $f(X) = (X - z)g(X)$, we obtain $f'(X) = g(X) + (X - z)g'(X)$, and evaluating at $X = z$, we get

$$f'(z) = g(z)$$

Consider $\{e_i^*\}_{i=0}^{n-1}$ the basis of B^* dual to $\{1, x, x^2, \dots, x^{n-1}\}$, and denote by τ the n-th dual basis element, that is, $\tau(z^i) = 1$ if $i = n-1$ and $\tau(z^i) = 0$ otherwise. We claim now that $b_i \tau = e_i^*$. To prove that, let's consider the rings $C := A[X]$, $D := A[X] \otimes_A B \cong B[X]$. D is a free C-module with basis $\{1 \otimes z^i\}_{i=0}^{n-1}$. Let's regard τ as a map $D \to C$, and denote by $\sigma : D \to C$ the $A[X]$-linear map defined by $z \mapsto X$. We claim that the following equality holds.

$$f(X)\tau(h(X)) = \sigma((X - z)h(X)) \quad \forall h \in D$$

Note that, to prove this equality, it will be enough to prove it for all the elements of the basis $h = 1 \otimes z^i$, for $i = 0, \dots, n-1$. We will split in two cases:

$\boxed{i < n-1}$ In that case, $h(X) = z^i$, and so $\tau(h) = 0$ and $f(X)\tau(h(X)) = 0$. On the other side, $\sigma((X - z)z^i) = X\sigma(z^i) - \sigma(z^{i+1}) = 0$ and so the equality holds.

$\boxed{i = n-1}$ In that case, $h(X) = z^{n-1}$, and so $\tau(h) = 1$ and $f(X)\tau(h(X)) = f(X)$. On the other side, $\sigma((X - z)z^i) = X\sigma(z^i) - \sigma(z^{i+1}) = XX^{n-1} - \sigma(-\sum_{j=1}^{n} a_j z^{n-j}) = f(X)$, and so the equality holds too for $i = n-1$.

So the equality above holds, and now we will apply it to the polynomial $h(X) = z^i \sum_{j=0}^{n-1} b_j X^j = z^i g(X)$. On the left hand side, we have $f(X)\tau(\sum_{j=0}^{n-1} z^i b_j X^j) = f(X) \sum_{j=0}^{n-1} X^j \tau(z^i b_j)$. On the right hand side, we have $\sigma((X-z)z^i \sum_{j=0}^{n-1} b_j X^j) = \sigma(z^i(X-z)g(X)) = \sigma(z^i f(X)) = f(X)X^i$, where in the last equality we have used that $f(X) \in A[X]$ and the $A[X]$-linearity of σ.

Now, equating terms of the same degree on both sides of the equality we must have $\tau(z^i b_j) = \delta_{ij}$. This finally proves that

$$b_i\tau = e_i^*$$

This formula allows to find a more useful expression for the trace map:

$$Tr_{B/A} = \sum_{i=0}^{n-1} e_i e_i^* = \sum_{i=0}^{n-1} z^i b_i \tau = g(z)\tau = f'(z)\tau$$

Therefore, taking into account that $\forall y \in B$, it can be written as $y = \sum_{i=0}^{n-1} c_i e_i = \sum_{i=0}^{n-1} e_i^*(y) e_i$, we have $f'(z)y = \sum_{i=0}^{n-1} f'(z)e_i^*(y)e_i = \sum_{i=0}^{n-1} b_i f'(z)\tau(y)z^i = \sum_{i=0}^{n-1} b_i Tr(y)z^i = \sum_{i=0}^{n-1} Tr(b_i y)z^i$. Then, if $(f, f') = 1$, that is, $f'(z)$ is a unit in B, then we can write

$$y = (f'(z))^{-1} \sum_{i=0}^{n-1} Tr(b_i y)z^i$$

Recall that proving that B is a separable A-algebra is equivalent to proving that the map $\varphi : B \mapsto \mathrm{Hom}_A(B, A)$ defined by $\varphi(y) : x \mapsto Tr(yx)$ is an A-module isomorphism. Consider the map $\psi : \mathrm{Hom}_A(B, A) \to B$ defined by $u \mapsto (f'(z))^{-1}(\sum_{i=0}^{n-1} u(b_i)z^i)$. It is clear that the composition $\psi \circ \varphi$ yields the identity, and so φ is injective.

On the other hand, every map $u \in B^*$ can be written as $u = \sum_{i=0}^{n} \alpha_i e_i^* = \sum_{i=0}^{n} \alpha_i b_i \tau = b_i f'(z)^{-1} Tr_{B/A}$. Therefore, the element $\sum_{i=0}^{n-1} \alpha_i b_i (f'(z))^{-1}$ is mapped to u by φ, and this proves that φ is surjective, and so B is a projective separable A-algebra (in particular a free separable A-algebra) □

For the example that we have just done, we do not need the notion of projective separable algebras, just the notion of free separable algebras. Just for completness, let's also give an example of a case that is projective separable but not free separable.

Example 3.3. Let A be a ring, and regard A as an A^2-algebra via the projection on the first coordinate $p_1 : A^2 \to A$. Then, A is a finite projective separable A^2-algebra.

Proof. It is finite, because it is generated by the element $1 \in A$. It is also projective, because A is a direct summand of A^2: $A \oplus A \cong A^2$. The difficult part to prove is the separability. To prove that, we need to consider some isomorphisms.

a) $A^* = \mathrm{Hom}_{A^2}(A, A^2) \cong A$, via the isomorphism

$$\begin{aligned} \theta : A \longrightarrow & A^* \\ b \longmapsto & \theta(b) : a \longmapsto (ab, 0) \end{aligned}$$

Note that the injectivity is trivial: Given $f_1, f_2 \in \mathrm{im}\theta$, $f_i = \theta(b_i)$, we have $b_1 = p_1(f_1(1)) = p_2(f_2(1)) = b_2$. As for the surjectivity, note that every element in A^* is completely determined by the image of $1 \in A$. Let $f \in A^*$, and $f(1) = (a, b) \in A^2$. By A^2 linearity, we must have $(a', b')f(1) = f(a')$, $\forall (a', b') \in A^2$. Taking $b' = 0$, $a' = 1$ we get $f(1) = (a, 0)$, so $f = \theta(a)$ and θ is surjective.

b) $\mathrm{Hom}_{A^2}(A, A) \cong A$ via the isomorphism

$$\begin{aligned} \sigma : A \longrightarrow & \mathrm{Hom}_{A^2}(A, A) \\ b \longmapsto & \theta(b) : a \longmapsto ab \end{aligned}$$

It is immediate to check that the map $\mathrm{Hom}_{A^2}(A, A) \to A$, $f \mapsto f(1)$ is the inverse of σ.

In order to be able to discuss if A is separable as an A^2-algebra, we need to determine what is the trace map.

The map $\phi_{A,A} : A^* \otimes_{A^2} A \to \mathrm{Hom}_{A^2}(A, A)$ sends an element $\theta(a) \otimes 1$ to $\phi_{A,A}(\theta(a) \otimes 1) : b' \mapsto \theta(a)(b')1 = ab'$, which is exactly the map $\sigma(a)$. Note that, as we saw on (a), the evaluation map $A^* \otimes_{A^2} A \to A^2$ has image $(A, 0)$, and sends $\theta(a) \otimes 1 \to (a, 0)$. Putting all this together, we see that $Tr_{A/A^2} : \mathrm{Hom}_{A^2}(A, A) \to A^2$ is defined by $\sigma(a) \mapsto (a, 0)$.

Therefore, $\varphi_A(a)$ is defined by $b \mapsto Tr_{A/A^2}(ab) = (ab, 0)$, and so $\varphi_A = \theta$, which we have already seen to be an isomorphism. □

4. The étale fundamental group

As it was said in the Introduction, the goal of this thesis is to prove that, given a connected scheme X, the category of its finite étale coverings is equivalent to the category of π-**sets** for a certain profinite group π. This chapter begins translating into geometric language the algebraic concepts of the previous chapter, in particular, it introduces *finite and locally free* morphisms of schemes, which correspond to finite projective algebras. It is also shown that finite étale morphisms (which are our objects of interest, and a particular case of finite and locally free morphisms) correspond to projective separable algebras. Then, we introduce the concept of totally split morphisms, which simplify the treatment of finite étale morphisms, and we finally prove the main theorem that gives rise to the construction of the étale fundamental group.

4.1 Moving from algebra to geometry

Let's begin with the reminder of some basic concepts of scheme theory.

Definition 4.1. Let $f : Y \to X$ be a morphism of schemes.

- f is *affine* if there exists a covering of X by open affine sets $U_i = \text{Spec}(A_i)$ such that $\forall i$, $f^{-1}(U_i)$ is also affine, $f^{-1}(U_i) = \text{Spec}(B_i)$.
- f is *finite* if there exists a covering of X by open affine sets $U_i = \text{Spec}(A_i)$ such that $\forall i$, $f^{-1}(U_i) = \text{Spec}(B_i)$, where B_i is a finite A_i-algebra.
- f is *finite and locally free* if there exists a covering of X by open affine sets $U_i = \text{Spec}(A_i)$ such that $\forall i$, $f^{-1}(U_i) = \text{Spec}(B_i)$, where B_i is a finitely generated and free as an A_i module.

It is immediate from the definitions that every finite morphism is in particular affine. It is well known that if $f : Y \to X$ is affine, $\forall U = \text{Spec}(A)$ open affine subset of X, $f^{-1}(U) = V = \text{Spec}(B)$ is affine. Similarly, if f is finite, $\forall U = \text{Spec}(A)$ open affine subset of X, $f^{-1}(U) = V = \text{Spec}(B)$ is a finite A-algebra (see Proposition A.3 and Proposition A.4 for proofs). For the case of locally free morphisms we do not have such a strong result. Instead, we have the following proposition, which is the geometric equivalent of Theorem 3.1, and states that finite and locally free morphisms of schemes correspond, when restricted to affines, to projective modules.

Proposition 4.1. Let $f : Y \to X$ be a morphism of schemes. f is finite and locally free $\iff$ for every open affine subset of X, $U = \text{Spec}(A)$, $f^{-1}(U) = \text{Spec}(B)$, where B is a finite projective A-algebra.

Proof. $\boxed{\Leftarrow}$ Take an open affine covering of X, and apply Theorem 3.1, $(i) \Rightarrow (iii)$ to show that the covering can be refined to find a locally free covering.

$\boxed{\Rightarrow}$ Suppose that f is finite and locally free. Let $\{U_i = \text{Spec}(A_i)\}$ be the covering of the definition, and let $U = \text{Spec}(A)$ be any open affine in X. As f is finite, $f^{-1}(U) = \text{Spec}(B)$ is affine. Restricting to smaller open sets $V_j \subset U \cap U_i$ for a certain $i \in I$, we can find a covering of U by affine open subsets $V_j = \text{Spec}(A_{f_j})$ such that $f^{-1}(V_j) = \text{Spec}(B_{f_j})$, with B_{f_j} an A_{f_j} algebra that is finitely generated and free as an A_{f_j}-module. Now using Theorem 3.1, $(iii) \Rightarrow (i)$, we conclude that B is a finite projective A-algebra. □

Given $f : Y \to X$ a finite and locally free morphism of schemes, on each open affine subset $U \subset X$, $U = \text{Spec}(A)$, the finite projective algebra B such that $f^{-1}(\text{Spec}(A)) = \text{Spec}(B)$, induces a continuous rank function $\mathrm{Spec}(A) \to \mathbb{Z}$ (Definition 3.5). This functions agree on the intersection of different affine open sets, so they can be extended to a function in the whole underlying topological space of X. This tells us that the following definition makes sense.

Definition 4.2. Given $f : Y \to X$, we call the *degree of* Y *over* X the function $\mathrm{sp}(X) \to \mathbb{Z}$ induced by the rank functions on each affine open subset of X. We denote it $[Y : X]$ or $\deg(f)$.

Observation 4.1. As the degree is a locally constant function, it is continuous when we give $\mathbb{Z}$ the discrete topology. Therefore, the set $\{x \in \mathrm{sp}(X) | [Y : X](x) = n\}$ is open and closed in X.

The following proposition shows how the degree tells us some properties of a finite and locally free morphism of schemes.

Proposition 4.2. Let $f : Y \to X$ be a finite and locally free morphism of schemes. Then,

i) $Y = \varnothing \iff [Y : X] = 0$

ii) $Y \to X$ is an isomorphism $\iff [Y : X] = 1$.

iii) $Y \to X$ is surjective $\iff [Y : X] \geq 1$ (i.e., for every open affine subset of X, $U = \mathrm{Spec}(A)$ we have $f^{-1}(U) = \mathrm{Spec}(B)$, with B a faithfully projective A-algebra)

Proof. As the notion of degree is local, we can restrict to affines and assume that $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$.

i) It is immediate, taking into account that $\mathrm{Spec}(B) = \varnothing \iff B = 0$.

ii) Taking into account the equivalence of categories between affine schemes and rings, The map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is an isomorphism if and only if $A \to B$ is an isomorphism. By Proposition 3.5 (iii), this happens if and only if $1 = [B : A] = [Y : X]$, and so this proves (ii).

iii) $\boxed{\Leftarrow}$ If $[B : A] \geq 1$, the map $A \to B$ is injective by Proposition 3.5 (i). Then A can be seen as a subring of B. As B is a finitely generated A-module, it is in particular integral over A, and [1], Theorem 5.10 says that $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.

$\boxed{\Rightarrow}$ Let $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{q}^c = \mathfrak{p}$. As the map is surjective, $B \neq 0$, and so $B_{\mathfrak{q}} \neq 0$ either. This implies that $B_{\mathfrak{p}} \neq 0$, and so $[B : A](\mathfrak{p}) \neq 0$. This holds $\forall \mathfrak{p} \in \mathrm{Spec}(A)$, so $[Y : X] = [B : A] \geq 1$.

□

Lemma 4.1. Let $f : Y \to X$ and $g : Z \to Y$ be finite and locally free morphisms of schemes. Then, $f \circ g$ is finite and locally free.

Proof. Let $U = \mathrm{Spec}(A)$ be an open affine subset of X. Then, as f is finite and locally free, $V = f^{-1}(U) = \mathrm{Spec}(B)$, with B a finite projective A-algebra. Similarly $g^{-1}(V) = (f \circ g)^{-1} = \mathrm{Spec}(C)$, and C is a finite projective B-algebra. Therefore, by Lemma 3.6, C is also a finite projective A-algebra, and so $f \circ g$ is finite and locally free. □

After these considerations on finite and locally free morphisms, let's recall the definition of our objects of interest: *finite étale* morphisms, which are a very special kind of finite and locally free morphisms.

Definition 4.3. A morphism of schemes $f : Y \to X$ is called *finite étale* if there exists a covering of X by open affine subsets $U_i = \mathrm{Spec}(A_i)$ such that $f^{-1}(U_i) = \mathrm{Spec}(B_i)$, where B_i is a free separable A_i-algebra. See Appendix A.3 for an alternative definition of finite étale morphisms.

The following proposition shows that, the same way that finite and locally free morphisms of schemes restricted to affine sets correspond to finite projective algebras, finite étale morphisms correspond to projective separable algebras

Proposition 4.3. Let $f : Y \to X$ be a morphism of schemes. f is finite étale $\iff$ for every open affine subset of X, $U = \mathrm{Spec}(A)$, $f^{-1}(U) = \mathrm{Spec}(B)$, where B is a projective separable A-algebra.

Proof. $\boxed{\Rightarrow}$ Let f be finite étale, it is in particular finite and locally free, so given $U = \mathrm{Spec}(A)$ open affine subset of X, $f^{-1}(U)$ will be affine, $f^{-1}(U) = \mathrm{Spec}(B)$ with B a finite projective A-algebra. Using [1], Proposition 3.9, we know that the map $\varphi_{B/A} : B \to \mathrm{Hom}_A(A, B)$ $\varphi_{B/A}(b) : x \mapsto Tr_{B/A}(bx)$ will be an isomorphism $\iff$ the corresponding maps on the stalks $(\varphi_{B/A})_{\mathfrak{p}} : B_{\mathfrak{p}} \to \mathrm{Hom}_A(A, B)_{\mathfrak{p}}$ are isomorphisms $\forall \mathfrak{p}$.

Using Lemma 3.3, it yields that $(\varphi_{B/A})_{\mathfrak{p}}$ will be isomorphisms if and only if the maps $\varphi_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}$ are isomorphisms, that is, if $B_{\mathfrak{p}}$ is a projective separable $A_{\mathfrak{p}}$ algebra for every $\mathfrak{p}$. But this is true as there is a covering of $\mathrm{Spec}(A)$ by affine open subsets $U_i = \mathrm{Spec}(A_{f_i})$ (maybe restricting the original cover) such that B_{f_i} is a projective separable A_{f_i} algebra.

$\boxed{\Rightarrow}$ As the preimage of every affine subset of X, $\mathrm{Spec}(A)$ is the spectrum of a projective A-algebra, the morphism is finite and locally free, so there is a covering $U_i = \mathrm{Spec}(A_i)$ of X such that $f^{-1}(U_i) = \mathrm{Spec}(B_i)$, where B_i is finitely generated and free as an A_i-module. Moreover, B_i is a projective separable A_i-algebra, and so in conclusion, B_i is a free separable A_i-algebra (Observation 3.4). □

4.2 Finite étale morphisms

We will now prove some properties of finite étale morphisms of schemes.

Lemma 4.2. Let $f_i : Y_i \to X$, $i \in \{1, \dots, n\}$ be morphisms of schemes. Let $Y := Y_1 \amalg \cdots \amalg Y_n$ and $f : Y \to X$ the morphism of schemes induced by $\{f_i\}$. Then,

i) f finite étale $\iff$ f_i finite étale $\forall i$.

ii) $[Y : X] = \sum_{i=1}^{n} [Y_i : X]$ if $Y \to X$ is finite and locally free.

Proof. i) $\boxed{\Leftarrow}$ Let U be an open affine set of X. Then, $(f_i)^{-1}(U) = \mathrm{Spec}(B_i)$ is also affine. Therefore we have

$$f^{-1}(\mathrm{Spec}(A)) = \coprod_{i=1}^{n} \mathrm{Spec}(B_i) \cong \mathrm{Spec}(\prod_{i=1}^{n} B_i)$$

Where the isomorphism comes from Proposition A.5. Then, the morphism f is also affine, and $\prod_{i=1}^{n} B_i$ is projective separable (Lemma 3.10).

$\boxed{\Rightarrow}$ Let $U = \mathrm{Spec}A$ be an open affine set. Then $f^{-1}(U) = \mathrm{Spec}(B)$ is also affine. But $\mathrm{Spec}(B)$ is disconnected, as the sets Y_i are open and closed in Y, so $\mathrm{Spec}(B) = \coprod_{i=1}^{n}(\mathrm{Spec}(B) \cap Y_i)$. Then, by Proposition A.5, $B \cong \prod_{i=1}^{n} B_i$ and $\mathrm{Spec}(B) \cong \coprod_{i=1}^{n} \mathrm{Spec}(B_i)$, $f_i^{-1}(U) = \mathrm{Spec}(B_i)$. Using again Lemma 3.10, it holds that each of the B_i is a projective separable algebra, so each f_i is finite étale.

ii) Note that the proof above also holds if we relax the finite étale condition to finite and locally free. Moreover, if we denote B, B_i as before, given $\mathfrak{p}$ an $A_{\mathfrak{p}}$ module, we have that $(B_i)_{\mathfrak{p}} \cong A_{\mathfrak{p}}^{n(i)}$ as A-modules and $B_{\mathfrak{p}} \cong \prod_{i=1}^{n}(B_i)_{\mathfrak{p}} \cong \prod_{i=1}^{n}(A_{\mathfrak{p}})^{n(i)} \cong (A_{\mathfrak{p}})^{\sum_{i=1}^{n} n(i)}$. Therefore the formula $[Y : X] = \sum_{i=1}^{n}[Y_i : X]$.

□

4.2.1 Base changes

The following proposition, which will be key in the verification of the axioms, tells us that the finite étale property is preserved if we make a base change.

Proposition 4.4 (Base change of a finite étale morphism)**.** Let $f : Y \to X$ be finite étale, and $g : W \to X$ any morphism of schemes. Then,

i) The map $p_2 : Y \times_X W \to W$ is finite étale.

ii) The diagram

$$\begin{tikzcd} sp(W) \arrow[r] \arrow[d, "deg(p_2)"'] & sp(X) \arrow[dl, "deg(f)"] \\ \mathbb{Z} & \end{tikzcd}$$

is commutative.

iii) If f is surjective, then $Y \times_X W \to W$ is also surjective.

Proof. i)

$$\begin{tikzcd} Y \times_X W \arrow[r, "p_2"] \arrow[d, "p_1"] & W \arrow[d, "g"] \\ Y \arrow[r, "f"] & X \end{tikzcd}$$

Let $\{U_i = \mathrm{Spec}(A_i)\}$ be an open affine cover of X such that $f^{-1}(U_i) = \mathrm{Spec}(B_i)$, B_i free separable A_i-algebra. If we restrict to each affine open set, we have that $(fp_1)^{-1}(U_i)$ is a fibred product for $g^{-1}(U_i)$ and $f^{-1}(U_i)$ over U_i

$$\begin{tikzcd} (fp_1)^{-1}(U_i) \arrow[r, "p_2"] \arrow[d, "p_1"] & g^{-1}(U_i) \arrow[d, "g"] \\ f^{-1}(U_i) \arrow[r, "f"] & U_i \end{tikzcd}$$

Let $\{V_{ij} = \mathrm{Spec}(C_{ij})\}$ be an affine open cover of $g^{-1}(U_i)$. By [3] Theorem II.3.3 Step 4 we have that $(fp_1)^{-1}(U_i) \cap p_2^{-1}(V_{ij})$ is a fibred product for $f^{-1}(U_i)$ and V_{ij} over U_i. But $U_i = \mathrm{Spec}(A_i)$, $f^{-1}(U_i) = \mathrm{Spec}(B_i)$, $V_{ij} = \mathrm{Spec}(C_{ij})$, and so we know that $\mathrm{Spec}(B_i \otimes_{A_i} C_{ij})$ is a fibred product. By uniqueness of the fibred product, we have then that

$$(gp_2)^{-1}(\mathrm{Spec}(A_i)) \cap p_2^{-1}(\mathrm{Spec}(C_{ij})) = p_2^{-1}(\mathrm{Spec}(C_{ij})) \cong \mathrm{Spec}(B_i \otimes_{A_i} C_{ij})$$

In conclusion, there is an affine open cover of W, namely $\{V_{ij}\}_{i,j}$ such that $p_2^{-1}(V_{ij}) = \mathrm{Spec}(B_i \otimes_{A_i} C_{ij})$ is affine. Moreover, if B is free projective as an A_i-algebra, then $B_i \otimes_{A_i} C_{ij}$ is free as a C_{ij}-module (by distribution of direct sum and tensor product). Moreover, using Proposition 3.8 $B_i \otimes_{A_i} C_{ij}$ is free separable as a C_{ij}-algebra. In conclusion, $p_2 : Y \times_X W \to W$ is a finite étale morphism.

ii) Let A_i, B_i, C_{ij} as in the proof of (i). Let $n(i)$ such that $B_i \cong A_i^{n(i)}$ as A_i-modules. Then, $B_i \otimes_{A_i} C_{ij} \cong C_{ij}^{n(i)}$ as C_{ij}-modules. Therefore, $\mathrm{rank}_{C_{ij}}(B_i \otimes_{A_i} C_{ij}) = \mathrm{rank}_{A_i}(B_i) = n(i)$. Localizing at every point, we obtain that the diagram of the statement is commutative.

iii) This is an immediate consequence of Proposition 4.2. Indeed, $f : Y \to X$ is surjective $\Rightarrow [Y : X] \geq 1$. But by (ii), also $[Y \times_X W : W] \geq 1$, and using Proposition 4.2 again $\Rightarrow Y \times_X W \to W$ is surjective. □

Observation 4.2. The same proof holds if we replace finite étale by the weaker condition of finite and locally free. Therefore, as a corollary we have that, if $f : Y \to X$ is finite and locally free, and $g : W \to X$ is any morphism of schemes, then

i) The map $p_2 : Y \times_X W \to W$ is finite and locally free.

ii) The diagram

$$\begin{tikzcd}
sp(W) \arrow[r] \arrow[d, "deg(p_2)"'] & sp(X) \arrow[dl, "deg(f)"] \\
\mathbb{Z} &
\end{tikzcd}$$

is commutative.

iii) If f is surjective, then $Y \times_X W \to W$ is also surjective.

We will see now that the condition for the reciprocal to hold is exactly that the extension is surjective, finite and locally free.

Observation 4.3. A morphism of schemes $Y \to X$ is surjective, finite and locally free $\iff$ $\forall U$ open affine subset of X, $f^{-1}(U) = \mathrm{Spec}B$, for B a faithfully projective A-algebra. This is an immediate consequence of Proposition 4.2 and Proposition 4.1.

Proposition 4.5. Let $f : Y \to X$ be an affine morphism of schemes, and $g : W \to X$ a morphism that is surjective, finite and locally free. Then, f is finite étale if and only if $Y \times_X W \to W$ is finite étale.

Proof. $\boxed{\Rightarrow}$ Holds in general (there's no need to require g to be surjective, finite and locally free), see Proposition 4.4.

$\boxed{\Leftarrow}$ Let $U = \mathrm{Spec}(A)$ be an affine open subset of X. As f is affine, $f^{-1}(U) = \mathrm{Spec}(B)$. Then, it will be enough to prove that B is projective separable over A. By the observation above, $g^{-1}(U) = \mathrm{Spec}(C)$ for a faithfully projective A-algebra C. Then, the inverse image of $\mathrm{Spec}(C)$ under $Y \times_X W \to W$ is $\mathrm{Spec}(B \otimes_A C)$ ([3], Theorem II.3.3). As $Y \times_X W \to W$ is finite étale, $B \otimes_A C$ is a projective separable C-algebra. Now using Proposition 3.7, we conclude that B is a projective separable A-algebra. □

4.2.2 Totally split morphisms

Definition 4.4. A morphism of schemes $f : Y \to X$ is called *totally split* if X can be written as a disjoint union of schemes $X = \coprod_{i=0}^{\infty} X_n$, such that $\forall n$ the scheme $f^{-1}(X_n)$ is isomorphic to the disjoint union of n copies of X_n, $f^{-1}(X_n) \cong \coprod_{i=1}^{n} X_n$.

In particular, totally split morphisms are finite étale: Indeed, if take an open affine cover of X such that every set $\mathrm{Spec}(A)$ of the covering is totally included in a disjoint piece X_n, we will have that its preimage is isomorphic to n disjoint copies of itself, $f^{-1}(\mathrm{Spec}(A)) = \coprod_{i=1}^{n} \mathrm{Spec}(A) = \mathrm{Spec}(A^n)$, and A^n is a projective separable A-algebra, as it is the product of projective separable A-algebras. We will see now that with a well-chosen base change every finite étale morphism can be reduced to a totally split one.

Proposition 4.6. Let $f : X \to Y$ be a morphism of schemes. Then, f is finite étale $\iff$ f is affine and there exists a surjective, finite and locally free morphism of schemes, $W \to X$ such that $Y \times_X W \to W$ is totally split.

Proof. $\boxed{\Leftarrow}$ If f is affine, and $Y \times_X W \to W$ is totally split, (in particular, finite étale) for a certain $W \to X$, surjective, finite and locally free, then Proposition 4.5 tells us that f is finite étale.

$\boxed{\Rightarrow}$ Let's assume now that $f : Y \to X$ is finite étale. First we will deal with the case where the degree is constant. Let $[Y : X] = n$. We have to construct a morphism $W \to X$ such that $Y \times_X W \to W$ is totally split. Let's proceed by induction on n. For the base case $n = 0$, we have $Y = \varnothing$, and so $Y \times_X W = \varnothing$ too. Therefore, taking for instance $W = X$ and $W \to X$ the identity morphism, which is surjective, finite and locally free, $Y \times_X W \to W$ corresponds to $\varnothing \to X$, which is totally split.

Now suppose that $n > 0$. Let's first prove that the diagonal morphism $d : Y \to Y \times_X Y$ (that is, the morphism induced by two identity maps $Y \to Y$) is both an open and a closed immersion. We will start with the affine case: As f is finite étale, if $X = \text{Spec}(A)$, then $Y = \text{Spec}(B)$, with B a projective separable A-algebra. By Theorem 3.2, $\exists$ an A-algebra C such that $B \otimes_A B \cong B \times C$ as B-algebras, and through this isomorphism the morphism of B-algebras $u : B \otimes_A B \to B$, $x \otimes y \to xy$ becomes the projection on the first coordinate. This map satisfies the following commutative diagram

$$\begin{tikzcd}
B & & \\
& B \otimes_A B \arrow[ul, dotted, "u"'] & B \arrow[l, "q_1"] \arrow[ull, bend right, "\text{id}"'] \\
& B \arrow[u, "q_2"] \arrow[uul, bend left, "\text{id}"] & A \arrow[l] \arrow[u]
\end{tikzcd}$$

Where the maps q_1, q_2 are defined as $x \mapsto x \otimes 1$ and $x \mapsto 1 \otimes x$. Through the anti-equivalence of categories between rings and affine schemes, this diagram corresponds to the diagram

$$\begin{tikzcd}
\text{Spec} B \arrow[dr, dotted, "d"] \arrow[drr, bend left, "\text{id}"] \arrow[ddr, bend right, "\text{id}"'] & & \\
& \text{Spec} B \times_{\text{Spec} A} \text{Spec} B \arrow[r, "p_1"] \arrow[d, "p_2"] & \text{Spec} B \arrow[d] \\
& \text{Spec} B \arrow[r] & \text{Spec} A
\end{tikzcd}$$

In conclusion, the map corresponding to u is exactly d when we apply the Spec functor. As u composed with the isomorphism $B \times C \cong B \otimes_A B$ is the projection on the first coordinate, therefore the composition

$$\text{Spec}(B) \xrightarrow{d} \text{Spec}(B \otimes_A B) \xrightarrow{\cong} \text{Spec}(B) \amalg \text{Spec}(C)$$

is the identity on Spec$B$, and therefore this is an open and closed mapping, and so must be d. This proves the affine case. In the general case, we can cover X by open affine subsets $\{U_i = \text{Spec}(A_i)\}$ so Y is covered by $\{f^{-1}(U_i) = \text{Spec}(B_i)\}$, and $Y \times_X Y$ is covered by $\text{Spec}(B_i \otimes_{A_i} B_i) \cong \text{Spec}(B_i) \amalg \text{Spec}(C_i)$. Then, the image of Y in $Y \times_X Y$ i open, as it is the union of the sets $\text{Spec}(B_i)$ in $\bigcup_i \text{Spec}(B_i) \amalg \text{Spec}(C_i)$, but also $Y \times_X Y \setminus d(Y)$ is open, as it is the union of the sets $\text{Spec}(C_i)$. In conclusion, $d : Y \to Y \times_X Y$ is an open and closed immersion.

Therefore, we can write $Y \times_X Y = Y \amalg Y'$ for a certain Y'. As f is finite étale, so is $Y \times_X Y \to Y$ (Proposition 4.4) and it also has constant degree n. Therefore, the same applies to the induced map $Y \amalg Y' \to Y$. As id : $Y \to Y$ has degree 1, then using Lemma 4.2 we know that $Y' \to Y$ (the restriction of $Y \amalg Y' \to Y$ to Y') will be finite étale of degree $n - 1$. Now we can apply the induction hypothesis on the map $Y' \to Y$, and so there exists a scheme W, and a morphism $g : W \to Y$ surjective, finite and locally free such that $Y' \times_Y W \to W$ is totally spit.

We will now prove that the composition $f \circ g : W \to X$ satisfies the property that we want. Note first that $Y \times_Y W \cong W$, and so the projection $Y \times_Y W \to W$ is totally split of rank 1. It is trivial that the direct sum of totally split morphisms is totally split, and so $(Y \times_Y W) \amalg (Y' \times_Y W) \to W$ is totally split. Then, the induced map $Y \times_X W \to W$ is also totally split:

$$Y \times_X W \cong Y \times_X (Y \times_Y W) \cong (Y \amalg Y') \times_Y W \cong (Y \times_Y W) \amalg (Y' \times_Y W) \to W$$

It should be checked that this chain of isomorphisms respects the projections to W. Take into account (as in [3], II, Proof of Theorem 3.3) that it will be enough to check that this holds locally on affine sets. Then, let $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$, $Y' = \mathrm{Spec}(B')$, $W = \mathrm{Spec}(C)$.

- $Y \otimes_X W \to W$ corresponds to the morphism of rings $C \to B \otimes_A C$ defined by $c \mapsto 1 \otimes c$.
- $Y \times_X W \cong Y \times_X (Y \times_Y W)$ corresponds to the isomorphism $B \otimes_A (B \otimes_B C) \to B \otimes_A C$ defined by $b \otimes (c \otimes c') \mapsto b \otimes cc'$.
- The isomorphism $Y \times_X (Y \times_Y W) \cong (Y \amalg Y') \times_Y W$ corresponds to a ring isomorphism $B \times B' \cong B \otimes_A B$, so $(1, 1) \mapsto 1 \otimes 1$.
- $(Y \amalg Y') \times_Y W \cong (Y \times_Y W) \amalg (Y' \times_Y W)$ corresponds to the ring isomorphism $(B \otimes_B C) \times (B' \otimes_B C) \to (B \times B') \otimes_B C$, defined by $(b \otimes c, b' \otimes c') \mapsto (b, b') \otimes cc'$
- $(Y \times_Y W) \amalg (Y' \times_Y W) \to W$ corresponds to the morphism of rings $C \to (B \otimes_B C) \times (B' \otimes_B C)$ defined by $c \mapsto ((1 \otimes c), (1 \otimes c))$.

Therefore, this diagram is commutative

$$\begin{tikzcd}
C \arrow[d] \arrow[rrrr] & & & & \\
(B \otimes_B C) \times (B' \otimes_B C) \arrow[r] & (B \times B') \otimes_B C \arrow[r] & B \otimes_A B \otimes_B C \arrow[r] & B \otimes_A C
\end{tikzcd}$$

as both paths send an element c to $1 \otimes c$. In conclusion, these canonical isomorphisms respect the projections, and this finishes the proof that the projection $Y \times_X W \to W$ is totally split.

Moreover, $[Y : X] \geq 1$, so $Y \to X$ is surjective. $W \to X$ is then the composition of surjective finite and locally free morphisms, so it is also surjective, finite and locally free (Lemma 4.1).

By now we have proven the case where $[Y : X] = n$ is constant. In the general case, let $X = \coprod_{i=0}^{\infty} X_n$, with $\mathrm{sp}(X_n) = \{x \in \mathrm{sp}(X) | [Y : X](x) = n\}$. Then $f^{-1}(X_n) \to X_n$ is finite étale of constant degree n, and so $\exists W_n \to X_n$ surjective, finite and locally free such that $Y_n \times_{X_n} W_n \to W_n$ is totally split. Then, the same holds for the induced map $\coprod_{i=0}^{\infty} W_n \to \coprod_{i=0}^{\infty} X_n$: This is trivial for the "totally split" and "surjective" conditions. It is also true for the "finite and locally free" condition as it is a local condition. □

As we will see in the following sections, the proposition we have just proven is key, as it will allow us to easily prove properties of finite étale morphisms by reducing to simpler case of totally split morphisms. But to be able to use the full potential of totally split morphisms, we still need to develop some results and properties about them.

Notation. Let X a scheme, and E a finite set, $\#E = n$. Then, we can write $X \times E$ to refer to the disjoint union of n copies of X. On the other hand, if A is a ring and E is a finite set, we will denote by A^E the ring of functions $E \to A$, with pointwise addition and product.

Lemma 4.3. i) Let X, Y be schemes, and E a finite set. There is a bijection between the set $\mathrm{Mor}_{\mathfrak{Sch}}(X \times E, Y)$ and the set of maps $E \to \mathrm{Mor}_{\mathfrak{Sch}}(X, Y)$.

ii) Let A be a ring, and let E be a finite set. Then $\mathrm{Spec}(A) \times E \cong \mathrm{Spec}(A^E)$.

iii) If A is a ring without non-trivial idempotents, and E, D are two finite sets, every A-algebra morphism $A^E \to A^D$ is induced by a map $D \to E$.

Proof. i) Consider a morphism $f : \coprod_E X \to Y$. If we restrict to each X, we get a collection of morphisms $\{f_i : X \to Y\}_{i \in E}$. Reciprocally, a map $E \to \mathrm{Mor}_{\mathfrak{Sch}}(X, Y)$ corresponds to a collection of maps $f_i : X \to Y$, one for each $i \in E$. At its turn, this induces a map $\coprod_E X \to Y$. Therefore we have a bijective correspondence as we wanted.

ii) Note that $\mathrm{Spec}(A) \times E \cong \coprod_E \mathrm{Spec}(A) \cong \mathrm{Spec}(\prod_E A)$ (c.f. Proposition A.5). On the other side, we have the isomorphism $\mathrm{Spec}(\prod_E A) \cong \mathrm{Spec}(A^E)$ induced by the isomorphism of rings corresponding to evaluation: $A^E \to \prod_E A$, $f \mapsto (f(e))_{e \in E}$. The composition of these isomorphisms yields $\mathrm{Spec}(A) \times E \cong \mathrm{Spec}(A^E)$.

iii) Using (ii), it is enough to prove that every morphism $\prod_E A \to \prod_D A$ is of that form. Let $u : \prod_E A \to \prod_D A$ be such a map, and let $\{e_i\}_{i \in E}$ be the canonical basis of $\prod_E A$. As u is a morphism of A-algebras, $u(e_i) = u(e_i^2) = u(e_i)^2$. As A doesn't have non-trivial idempotents, the images of the basis elements must have either a 0 or a 1 on each coordinate. Apart from that, if we have $u(e_i)$ and $u(e_j)$ having a 1 in the same coordinate, then we reach a contradiction, as $0 = u(0) = u(e_i e_j) = u(e_i)u(e_j) \neq 0$. Then, $\forall d \in D$, $\exists$ at most one element $i \in E$ such that $u(e_i)_d = 1$. Moreover, as $\sum_{i \in E} u(e_i) = u(1) = 1$, we conclude that $\forall d \in D$ $\exists! i \in E$ such that $u(e_i)_d = 1$. Therefore, u is totally determined by the map $D \to E$ that sends each $d \in D$ to the element $i \in E$ such that $u(e_i)_d = 1$.

□

Proposition 4.7. Let X, Y, Z be schemes, and $f : Y \to X$, $g : Z \to X$ totally split morphisms of schemes. Let $h : Y \to Z$ satisfying $f = gh$. Then, $\forall x \in X$ there is an open affine neighbourhood U of x such that f, g, h are *trivial above* U, that is, there are finite sets D, E and isomorphisms $\alpha : f^{-1}(U) \to U \times D$, $\beta : g^{-1}(U) \to U \times E$, and a map $\phi : D \to E$ such that the following diagram commutes.

$$\begin{tikzcd}
f^{-1}(U) \arrow[rrr, "h"] \arrow[dd, "f"'] \arrow[dr, "\alpha"', "\cong"] & & & g^{-1}(U) \arrow[dd, "g"] \arrow[dl, "\beta"', "\cong"] \\
& U \times D \arrow[r, "\mathrm{id}_U \times \phi"] \arrow[dl] & U \times E \arrow[dr] & \\
U \arrow[rrr, "\mathrm{id}_U"] & & & U
\end{tikzcd}$$

Proof. Restricting to a neighbourhood of x, we can assume that $X = \mathrm{Spec}(A)$ and that f and g are both of them of constant degree. Then, $Y \xrightarrow{\cong} X \times D \cong \mathrm{Spec}(A^D)$ and $Z \xrightarrow{\cong} X \times E \cong \mathrm{Spec}(A^E)$, for certain finite sets E, D. (we have used here the isomorphisms of Lemma 4.3 (ii)). Then, we only have to find an open set $U \subset X$ such that the A-algebra homomorphism $A^E \to A^D$ corresponding to h is induced by a map $\phi : D \to E$ on U. Taking into account Lemma 4.3 (iii), it will be enough to prove that there is an open affine set $U \subseteq X$ such that $U = \mathrm{Spec}(A')$ and A' doesn't have trivial idempotents. As local rings don't have non-trivial idempotents (Proposition A.6), the map in the stalks $f_x^* : A_x^E \to A_x^D$, is induced by a map $\phi : D \to E$. Then, ϕ induces a map $\psi : A^E \to A^D$, that, when it is localized and viewed through the isomorphism of Lemma 3.3 yields the map $f_x^* : A_x^E \to A_x^D$. This equality as morphisms in the stalks can be lifted to a certain open set, that is, $\exists a \in A$, a not belonging to the prime ideal corresponding to the point x, such that f^* and ψ yield the same map in $A[1/a]^E \to A[1/a]^D$. Then, $U = \mathrm{Spec}(A[1/a])$ is the open affine set that we wanted. □

4.3 The category FEt_X

Definition 4.5. Let X be a scheme. Let's remind that the category of *finite étale coverings of X* is defined as follows

- **Objects**: Finite étale morphisms of schemes with target X.
- **Morphisms**: Given two objects $f : Y \to X$ and $g : Y' \to X$, a morphism from f to g is a morphism of schemes $h : Y \to Y'$ satisfying $f = gh$, i.e. making commutative the diagram $$\begin{tikzcd} Y \arrow[r, "h"] \arrow[d, "f"] & Y' \arrow[dl, "g"] \\ X & \end{tikzcd}$$

From now on, we will denote this category by $\mathbf{FEt}_X$.

Recall that the main theorem that we want to prove is the following one:

Theorem 4.1 (Main Theorem of Galois Theory for Schemes)**.** *Let X be a connected scheme. Then there exists a profinite group π, uniquely determined up to isomorphism, such that the category $\mathbf{FEt}_X$ of finite étale coverings of X is equivalent to the category π-**sets** of finite sets on which π acts continuously.*

It should be noted that, as a consequence of Theorem 2.1, to prove the main theorem it will be enough to see that that $\mathbf{FEt}_X$ is an essentially small Galois Category. Therefore, we need to find a fundamental functor and check that all the axioms of a Galois Category are satisfied. As we will see, this process is greatly simplified if we deal with totally split morphisms, by making base extensions by maps $W \to X$ that are surjective, finite and locally free. In the following, we will use this technique to prove some properties of finite étale morphisms and $\mathbf{FEt}_X$.

Proposition 4.8 (Composition of finite étale morphisms)**.** Let $g : Z \to Y$ and $f : Y \to X$ be finite étale morphisms of schemes. Then the composed morphism $Z \to X$ is finite étale.

Proof. First assume that f is totally split of constant degree n: $Y \cong X \amalg \cdots \amalg X$. Then, we can take the the preimage by g of each of the direct summands of Y that are isomorphic to X, and write $Z = Z_1 \amalg \cdots \amalg Z_n$, and it is immediate (as finite étale can be checked as a local property) that $Z_i \to X$ is finite étale for each i. Then, when we glue, the corresponding map $Z_1 \amalg \cdots \amalg Z_n \to X$, which is exactly $f \circ g$, is finite étale. The same argument now holds if f is totally split of non constant degree, as we can split it as a direct sum of totally split morphisms of constant degree.

In the general case, choose $W \to X$ such that $Y \times_X W \to W$ is totally split. Then, if we tensor with the map $Z \to Y$, we obtain a morphism $Z \times_Y (Y \times_X W) \cong Z \times_X W \to Y \times_X W$ which has to be finite étale by Proposition 4.4. Then, by the case dealt above, the composition $Z \times_X W \to Y \times_X W \to W$ is finite étale, and this map is exactly the projection $Z \times_X W \to W$, corresponding with the maps $f \circ g$ and $W \to X$. Therefore, by Proposition 4.5, $Z \to X$ is also finite étale. □

Lemma 4.4. Let $g : Z \to X$ and $f : Y \to X$ be affine morphisms of schemes, and suppose that we have a morphism $h : Y \to Z$ making a commutative diagram with f and g, i.e. $f = gh$. Then h is also affine.

Proof. Let $\{U_i\}$ be an affine open cover of X. Then $g^{-1}(U_i) = V_i$ is affine and $f^{-1}(U_i) = W_i$ is affine. Therefore, the sets $\{V_i\}$ form an affine open cover of Z such that $h^{-1}(V_i) = h^{-1}g^{-1}(U_i) = f^{-1}(U_i) = W_i$ are affine. Therefore f is affine. □

Proposition 4.9. Let $f : Y \to X$, $g : Z \to X$ be finite étale morphisms of schemes. Let $h : Y \to Z$ satisfying that $f = gh$. Then h is finite étale. In other words, given a scheme X, morphisms in the category $\mathbf{FEt}_X$ are in particular finite étale morphisms of schemes.

Proof. If f and g are totally split, we can select a covering by open affine sets of X such that f, g are trivial in the sense of Proposition 4.7. Let $U = \operatorname{Spec}(A)$ be one of the sets of this covering. Then $h : U \times D \to U \times E$ is induced by a map $\phi : D \to E$, and so $\forall e \in E$, we have that $h^{-1}(\beta^{-1}(U \times \{e\})) = \alpha^{-1}(\coprod_{d \in \phi^{-1}(e)} U) = \alpha^{-1}(\coprod_{d \in \phi^{-1}(e)} \operatorname{Spec}(A)) \cong \alpha^{-1}(\operatorname{Spec}(\prod_{d \in \phi^{-1}(e)} A))$. And, as $\prod_{d \in \phi^{-1}(e)} A$ is a finite projective separable A-algebra, this proves that h is finite étale.

Now let's deal with the general case in which f and g are not totally split. Let's choose surjective, finite and locally free morphisms $W_1 \to X$ and $W_2 \to X$ such that $Y \times_X W_1 \to W_1$ and $Z \times_X W_2 \to W_2$ are totally split. Then, by Observation 4.2 and Lemma 4.1, the morphism $W := W_1 \times_X W_2 \to X$ is also surjective, finite and locally free. We claim that this morphism makes both $f' : Y \times_X W \to W$ and $g' : Z \times_X W \to W$ totally split. Indeed, let $W_1 = \coprod_{i=0}^{\infty} W_{1i}$ such that $f^{-1}(W_{1i}) = W_{1i} \amalg \dots_{\text{i times}} \amalg W_{1i}$. Then, consider $W = (\coprod_{i=0}^{\infty} W_{1i}) \times_X W_2 \cong \coprod_{i=0}^{\infty}(W_{1i} \times_X W_2)$, and the preimage of each of the sets $(W_{1i} \times_X W_2)$ is $Y \times_X (W_{1i} \times_X W_2) = \coprod_{\text{i times}}(W_{1i} \times_X W_2)$. This proves that f' is totally split, and the same argument with W_2 shows that g' is totally split and the claim is proved.

By the properties of the fibred product, h induces a morphism $h' : Y \times_X W \to Z \times_X W$: If we denote $s : W \to X$ and $p : Y \times_X W \to Y$, we have $sf' = fp = (gh)p = g(hp)$.

$$\begin{tikzcd}
Y \times_X W \arrow[dr, dotted, "h'"] \arrow[drr, bend left, "f'"] \arrow[ddr, bend right, "h \circ p"'] & & \\
& Z \times_X W \arrow[r, "g'"] \arrow[d, "q"] & W \arrow[d, "s"] \\
& Z \arrow[r, "g"] & X
\end{tikzcd}$$

Then, we have totally split morphisms $f' : Y \times_X W \to W$, $g' : Z \times_X W \to W$ and a morphism h' satisfying that $f' = g'h'$ so, by the case proved above, h' is finite étale.

We already know that h is affine by the Lemma 4.4 above. As $W \to X$ is surjective, finite and locally free, then the morphism $q : Z \times_X W \to Z$ is also surjective, finite and locally free by base change. When we base change h by q, we obtain exactly the map $h' : Y \times_X W = Y \times_Z (Z \times_X W) \to (Z \times_X W)$, which is finite étale. Therefore, Proposition 4.5 implies that h is finite étale. □

The following results will characterize monomorphisms and epimorphisms in the category $\mathbf{FEt}_X$. It is important to note that a morphism h in the category $\mathbf{FEt}_X$ is a monomorphism or an epimorphism in $\mathbf{FEt}_X$ if and only if it is a monomorphism or an epimorphism when regarded in the category of schemes.

Proposition 4.10. Let $f : Y \to X$ and $g : Z \to X$ be finite étale morphisms, and let $h : Y \to X$ a morphism from f to g in $\mathbf{FEt}_X$, that is, $f = gh$. Then, h is an epimorphism in $\mathbf{FEt}_X$ if and only if h is surjective.

Proof. $\boxed{\Rightarrow}$ We know that h is finite étale, and therefore the set $Z_0 = \{z \in Z | [Y : Z](z) = 0\}$ is open and closed in Z, and we have that $h^{-1}(Z_0) = \varnothing$. Then, let's write $Z = Z_0 \amalg Z'$, and consider the morphisms $f_1, f_2 : Z_0 \amalg Z' \to Z_0 \amalg Z_0 \amalg Z'$ mapping the points of Z_0 to the first and second copies of Z_0, respectively. It's clear that $f_1 \circ h = f_2 \circ h$, and so this implies that $f_1 = f_2$, which is true only if $Z_0 = \varnothing$. Therefore $[Y : Z] \geq 1$ and so h is surjective by Proposition 4.2.

$\boxed{\Leftarrow}$ Suppose that we have $p, q : Z \to W$ such that $ph = qh$. We have to prove that $p = q$, and so it will be enough to check it locally, so we can assume that $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$, $Z = \mathrm{Spec}(C)$ and $W = \mathrm{Spec}(D)$. Let p, q, h correspond to maps $p', q' : D \to C$, $h' : C \to B$. If h is surjective, then by Proposition 4.2 we have that $[B : C] \geq 1$. By Proposition 3.5 this means that $h' : C \to B$ is an injective morphism of rings, and so $h'p' = h'q' \Rightarrow p' = q'$. This proves that $p = q$ and h is an epimorphism. □

Lemma 4.5. An open immersion is a monomorphism in the category of all schemes.

Proof. Let $f : Y \to X$ be an open immersion. f induces an isomorphism of Y with an open subscheme $U \subseteq X$. Let's denote $f|_U^{-1} : U \to Y$ the inverse map. Let $g, h : Z \to Y$ satisfying that $fg = fh$. Note that $\mathrm{im}(fg), \mathrm{im}(fh) \subseteq U$, and therefore, we can apply $f|_U^{-1}$ and we get $f|_U^{-1}fg = f|_U^{-1}fh \Rightarrow g = h$. In conclusion f is a monomorphism. □

Proposition 4.11. Let $f : Y \to X$ and $g : Z \to X$ be finite étale morphisms, and let $h : Y \to X$ a morphism from f to g in $\mathbf{FEt}_X$, that is, $f = gh$. Then, h is a monomorphism in $\mathbf{FEt}_X$ if and only if h is both an open and closed immersion.

Proof. $\boxed{\Leftarrow}$ This is trivial by the lemma above.

$\boxed{\Rightarrow}$ As $h : Y \to Z$ is a monomorphism, then $Y \times_Z Y \to Y$ is an isomorphism. This follows from the proof of Lemma 2.2 (note that in that proof, we only make use of the existence of fibred products, and so the arguments there are valid in the category of schemes). When we restrict to open affine sets $U = \mathrm{Spec}(A) \subseteq X$, $f^{-1}(U) = \mathrm{Spec}(B)$, $g^{-1}(U) = \mathrm{Spec}(C)$, this yields an isomorphism $B \cong B \otimes_C B$ sending $b \mapsto b \otimes 1$. Therefore, by Proposition 3.5 we must have $[B : C] \leq 1$. As this holds for every affine, we have $[Y : Z] \leq 1$. Then, $Z = Z_0 \amalg Z_1$, with $h^{-1}(Z_0) = \varnothing$, and so h induces an isomorphism of Y with Z_1, and therefore h is an open and closed immersion.

□

Observation 4.4. These results can be summarized in terms of the degree. Let $h : Y \to Z$ a morphism in $\mathbf{FEt}_X$. Then,

- h is a monomorphism $\iff$ $[Y : Z] \leq 1$.
- h is an epimorphism $\iff$ $[Y : Z] \geq 1$.

In particular, this characterization of monomorphisms implies that an object $Z \to X$ is connected in $\mathbf{FEt}_X$ (in the sense of Definition 2.3) if and only if $\mathrm{sp}(Z)$ is connected as a topological space. Indeed, if $\mathrm{sp}(Z)$ is connected, a monomorphism $Y \to Z$ has either $[Y : Z] = 1$ or $[Y : Z] = 0$. The first case corresponds to the identity subobject and the second one to the initial subobject, and these are the only possibilities. Reciprocally, suppose that $\mathrm{sp}(Z)$ is not connected. Then, $Z = Z_1 \amalg Z_2$ and the natural inclusion $Z_1 \to Z$ is a monomorphism different from $0, \mathrm{id}$, which is a contradiction.

4.3.1 Quotients under group actions

Finally, for a scheme X, we want to study quotients under group actions in $\mathbf{FEt}_X$. To do that, we will consider first the larger category $\mathbf{Aff}_X$, which is defined in a very similar manner.

Definition 4.6. Let X be a scheme. The category of $\mathbf{Aff}_X$ of affine morphisms with target X is defined as follows:

- **Objects**: Affine morphisms of schemes with target X.
- **Morphisms**: Given two objects $f : Y \to X$ and $g : Y' \to X$, a morphism from f to g is a morphism of schemes $h : Y \to Y'$ satisfying $f = gh$, i.e. making commutative the diagram $$\begin{tikzcd} Y \arrow[r, "h"] \arrow[d, "f"] & Y' \arrow[dl, "g"] \\ X & \end{tikzcd}$$

Proposition 4.12. Let X be a scheme. Then, for any object in $\mathbf{Aff}_X$, the quotient by a finite group of automorphisms exists in $\mathbf{Aff}_X$.

Proof. It will be useful to take into account the following lemma.

Lemma 4.6. Let X be a scheme. Then, the category $\mathbf{Aff}_X$ is anti-equivalent to the category of quasi-coherent sheaves of $\mathcal{O}_X$-algebras. [See Proposition A.7 for a proof of this lemma].

Let $\mathcal{A}$ be a quasi-coherent sheaf of $\mathcal{O}_X$-algebras, and G a finite group of automorphisms of $\mathcal{A}$. Given an open subset $U \subset X$, the set $\mathcal{A}(U)^G$ of G-invariants of $\mathcal{A}(U)$ is a sub-$\mathcal{O}_X(U)$-algebra of $\mathcal{A}(U)$, which is exactly the kernel of the map

$$\mathcal{A}(U) \to \bigoplus_{\sigma \in G} \mathcal{A}(U)$$
$$a \mapsto (\sigma(a) - a)_{\sigma \in G}$$

Therefore, by [3] Proposition II.5.7, the assignment $U \mapsto \mathcal{A}(U)$ defines a quasi-coherent sheaf of $\mathcal{O}_X$-algebras, that we denote by $\mathcal{A}^G$. For every $f : \mathcal{B} \to \mathcal{A}$ such that $\sigma \circ f = f$, $\forall \sigma \in G$, f factors through $\mathcal{A}^G$ via the inclusion $\mathcal{A}^G \to \mathcal{A}$. Passing to the anti-equivalent category of $\mathbf{Aff}_X$ again, this means that for a given $f : Y \to X \in Ob(\mathbf{Aff}_X)$ and G a finite group of automorphisms of f such that $f\sigma = f$, there exists the quotient of f by G, that is a morphism $g : Y/G \to X$ such that for every morphism $h : Y \to Z$ such that $h\sigma = h \, \forall \sigma \in G$, h factors through g. □

It is important to note, as we will need it later, that this construction shows also that $g^{-1}(U) = f^{-1}(U)/G$ for every open set $U \subseteq X$. Moreover, if we choose an open affine set $U = \text{Spec}(A)$, and let $f^{-1}(U) = \text{Spec}(B)$, then $g^{-1}(U) = \text{Spec}(B^G)$. We should remark also that our goal is to prove the existence of quotients by finite groups of automorphisms in $\mathbf{FEt}_X$. In account of Proposition 4.12, to do this it will be enough to show that the morphism $Y/G \to X \in \mathbf{Aff}_X$ is in fact finite étale. We will first need an auxiliary result.

Lemma 4.7. Let $f : Y \to X$ be an affine morphism, and let G be a finite group of automorphisms of f in $\mathbf{Aff}_X$. Let $W \to X$ be a finite and locally free morphism. Then, $(Y \times_X W)/G \to W$ is isomorphic to $(Y/G) \times_X W \to W$ in $\mathbf{Aff}_W$.

Proof. The morphism $Y \times_X W \to W$ is affine: This can be deduced using the same argument as in the proof of Proposition 4.4. It's easy to deduce from the properties of fibred products that G induces a group of automorphisms of $Y \times_X W \to W$ as follows: Denote p_1, p_2 the projections of $Y \times_X W$ to Y and W respectively. $\forall \sigma \in G$, consider the automorphism $\sigma' : Y \times_X W \to Y \times_X W$ corresponding to the morphisms $\sigma \circ p_1 : Y \times_X W \to Y$ and p_2, which make a commutative diagram with f and $W \to X$ because $f\sigma = f$.

$$\begin{tikzcd}
Y \times_X W \arrow[drr, bend left, "p_2"] \arrow[dr, dotted, "\sigma'"] \arrow[ddr, bend right, "\sigma \circ p_1"'] & & \\
& Y \times_X W \arrow[r, "p_2"] \arrow[d, "p_1"] & W \arrow[d] \\
& Y \arrow[r, "f"] & X
\end{tikzcd}$$

This construction allows us to regard G as a finite group of automorphisms of $Y \times_X W \to W$, and with a little abuse of notation we can talk about $(Y \times_X W)/G$ as the statement does. Where this may cause confusion we will denote G' to refer to the group of automorphisms of $Y \times_X W \to W$.

Let's denote $g : Y \to Y/G$ the natural map of passage to the quotient. In a similar way as we did with the automorphisms $\sigma \in G$, we can induce a morphism $g' : Y \times_X W \to (Y/G) \times_X W$:

$$\begin{tikzcd}
Y \times_X W \arrow[drr, bend left, "p_2"] \arrow[dr, dotted, "g'"] \arrow[ddr, bend right, "g \circ p_1"'] & & \\
& (Y/G) \times_X W \arrow[r] \arrow[d, "q"] & W \arrow[d] \\
& Y/G \arrow[r, "g"] & X
\end{tikzcd}$$

The morphism g' satisfies $g'\sigma' = g' \; \forall \sigma' \in G'$. This is true because $g'\sigma'$ corresponds to the morphism induced by $p_2\sigma' = p_2$ and $g\sigma p_1 = gp_1$. Therefore, by the universal property of the quotient, g' factors through $(Y \times_X W)/G$, that is, there is a morphism of schemes $\theta : (Y \times_X W)/G \to (Y/G) \times_X W$ that makes commutative the diagram

$$\begin{tikzcd}
Y \times_X W \arrow[r, "g'"] \arrow[d] & (Y/G) \times_X W \\
(Y \times_X W)/G \arrow[ur, dotted, "\theta"] &
\end{tikzcd}$$

. In particular θ respects the projection maps to W, so to prove that $(Y \times_X W)/G \to W$ is isomorphic to $(Y/G) \times_X W \to W$ in $\mathbf{Aff}_W$ it will be enough to prove that θ is an isomorphism. This can be checked locally, so we can assume that $X = \operatorname{Spec}(A)$, $Y = \operatorname{Spec}(B)$ and $W = \operatorname{Spec}(C)$, with C a finite projective A-algebra. We have to check that $B^G \otimes_A C \to (B \otimes_A C)^G$ is an isomorphism. Indeed, we have the exact sequence

$$0 \to B^G \to B \to \bigoplus_{\sigma \in G} B \to 0$$

As C is a finite projective A-algebra, and in particular flat, when we tensor with C we obtain an exact sequence

$$0 \to B^G \otimes_A C \to B \otimes_A C \to \bigoplus_{\sigma \in G} B \otimes_A C \to 0$$

This shows that $B^G \otimes_A C \cong (B \otimes_A C)^G$, which completes the proof. □

Proposition 4.13. Let $f : Y \to X$ be finite étale, and G a finite group of automorphisms of f in $\mathbf{FEt}_X$. Then, the quotient of f by G, $Y/G \to X$, exists in $\mathbf{FEt}_X$.

Proof. As we already remarked before, finite étale morphisms are in particular affine, so $g : Y/G \to X$ exists in $\mathbf{Aff}_X$, and so it will be enough to check that g is finite étale. First consider the case in which f is totally split. As G is a finite group, we can find an open cover of X by open sets $\{U_i\}$ such that the action every $\sigma \in G$ is trivial above $\{U_i\}$. Let U be one of the sets of this covering. Therefore, every $\sigma \in G$ is induced on U by a permutation $\phi_\sigma : D \to D$, where D is the finite set such that $f^{-1}(U) = U \times D$. Therefore, we can consider $U \times D/G$, which is a quotient of $U \times D$ under G in $\mathbf{Aff}_U$ (we are again making some abuse of notation: when we write D/G we mean the set of orbits of D under the group $\{\phi_\sigma\}_{\sigma \in G}$). Therefore $U \times D/G \cong f^{-1}(U)/G \cong g^{-1}(U)$, and so $g^{-1}(U) \to U$ is totally split, and in particular finite étale. As being finite étale is a local property, we conclude that $g : Y/G \to X$ is finite étale.

In the general case, take a surjective, finite and locally free morphism $W \to X$ such that $Y \times_X W \to W$ is totally split. By the case already proven, $(Y \times_X W)/G \to W$ is finite étale (we use here the same abuse of notation of G already explained in Lemma 4.7). By Lemma 4.7, $(Y/G) \times_X W \to W$ is also finite étale. Therefore the original morphism $g : Y/G \to X$ was already finite étale by Proposition 4.5. □

We will prove a last result about quotients in $\mathbf{FEt}_X$, which can be seen as a (stronger) version of Lemma 4.7 in $\mathbf{FEt}_X$.

Proposition 4.14. Let $f : Y \to X$ be a finite étale morphism, and let G be a finite group of automorphisms of f in $\mathbf{FEt}_X$. Let $h : Z \to X$ be any morphism of schemes. Then, $(Y \times_X Z)/G \to Z$ is isomorphic to $(Y/G) \times_X Z \to Z$ in $\mathbf{FEt}_Z$.

Proof. Consider the morphism $(Y \times_X Z)/G \to (Y/G) \times_X Z$ constructed as in the proof of Lemma 4.7. As usual, we will first deal with the case in which f is totally split. In that situation, we can cover X by open sets such that the action of every $\sigma \in G$ is trivial above every set of the covering. Therefore, for every open set U in the covering, $f^{-1}(U) \cong U \times D$, and $g^{-1}(U) \cong f^{-1}(U)/G \cong U \times (D/G)$. If we denote $h^{-1}(U) =: V$, we have that the preimage of V by the morphisms $(Y \times_X Z)/G \to Z$ and $(Y/G) \times_X Z \to Z$ is in both cases isomorphic to $V \times (D/G)$. This proves that $(Y \times_X Z)/G \to (Y/G) \times_X Z$ is locally an isomorphism, which is enough to conclude that it is an isomorphism.

In the general case, we choose a surjective, finite and locally free base extension $W \to X$ such that $Y \times_X W \to W$ is totally split. Then, consider the morphism $Z \times_X W \to W$. Applying the case already proven, we know that

$$((Y \times_X W) \times_W (Z \times_X W))/G \cong (Y \times_X W)/G \times_W (Z \times_X W) \tag{2}$$

By associativity and commutativity of fibred products we also have the following isomorphism:

$$(Y \times_X W) \times_W (Z \times_X W) \cong (Y \times_X Z) \times_Z (W \times_X Z) \tag{3}$$

Finally, we know that $W \times_X Z \to Z$ is surjective, finite and locally free by Observation 4.2.

Putting everything together, we have the following isomorphisms:

$$\begin{aligned}(Y \times_X Z)/G \times_Z (W \times_X Z) &\cong_{4.7 \text{ and } 3} ((Y \times_X W) \times_W (Z \times_X W))/G \cong_2 (Y \times_X W)/G \times_W (Z \times_X W)\\ &\cong_{4.7} ((Y/G) \times_X W) \times_W (Z \times_X W) \cong_3 (Y/G \times_X Z) \times_Z (W \times_X Z)\end{aligned}$$

And, in conclusion, $(Y \times_X Z)/G \times_Z (W \times_X Z) \to (W \times_X Z)$ is isomorphic to $((Y/G) \times_X Z) \times_Z (W \times_X Z) \to (W \times_X Z)$ in $\mathbf{FEt}_Z$. In other words, our morphism $(Y \times_X Z)/G \to (Y/G) \times_X Z$ becomes an isomorphism after tensoring with $\times_Z(W \times_X Z)$. Recall that $W \times_X Z \to Z$ is finite, surjective and locally free. If we look at this situation locally, we can take $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$, $Z = \mathrm{Spec}(C)$, $W = \mathrm{Spec}(D)$, and we have that $D \otimes_A C$ is a faithfully projective A-algebra, and that $(B^G \otimes_A C) \to (B \otimes C)^G$ becomes an isomorphism after tensoring with $D \otimes_A C$, that is, $(B \otimes_A C)^G \otimes_C (D \otimes_A C) \cong (B^G \otimes C) \otimes_C (D \otimes_A C)$. The fact that faithfully projective algebras are faithfully flat (Proposition 3.4) allows us to conclude that $(B^G \otimes_A C) \to (B \otimes C)^G$ was already an isomorphism after tensoring, which in scheme language means that the morphism $(Y \times_X Z)/G \to (Y/G) \times_X Z$ is locally an isomorphism, (which is enough to conclude that it is an isomorphism). □

4.4 Proof of the main theorem

We will now prove Theorem 4.1, by checking that all the axioms of Galois Categories are satisfied. It should be noted that most of the work has already been done in the previous section, when we treated the basic properties of the category $\mathbf{FEt}_X$.

Proof. Fix X a connected scheme. For every affine subset of $X \supset U = \mathrm{Spec}(A)$, we can consider the set of projective separable algebras over A. This is a set, and so the product of these sets ranging over all affine subsets of X is also a set. The objects in $\mathbf{FEt}_X$ can be regarded as a subset of this product (precisely the subset that can be glued to form a coherent covering). This proves that the objects in $\mathbf{FEt}_X$ form a set, and so $\mathbf{FEt}_X$ is essentially small. Let's proceed to check that it is a Galois Category.

G1 Terminal object: $\mathrm{id} : X \to X$ is a terminal object in $\mathbf{C}$, as for every $f : Y \to X$, the diagram

$$\begin{tikzcd} Y \arrow[r, "f"] \arrow[d, "h"] & X \arrow[dl, "\mathrm{id}"] \\ X & \end{tikzcd}$$ is commutative $\iff h = f$.

Fibred product: We already know that fibred products exist in the category of schemes. Suppose that we have $Y \to W$ and $Z \to W$ morphisms in $\mathbf{FEt}_X$, that is, we have the commutative diagram

$$\begin{tikzcd} Y \arrow[r] \arrow[dr] & W \arrow[d] & Z \arrow[l] \arrow[dl] \\ & X & \end{tikzcd}$$

. Then we claim that $Y \times_W Z \to X$, together with projections $Y \times_W Z \to Y$ and $Y \times_W Z \to Z$ is a fibred product for $Y \to X$ and $Z \to X$ over $W \to X$. Indeed, the universal property is immediately satisfied by the universal property of fibred products of schemes. Moreover, $Y \times_W Z \to X$ is finite étale because $Y \to W$ and $Z \to W$ are finite étale as they're morphisms in $\mathbf{FEt}_X$ (Proposition 4.9). The projection morphisms are then finite étale, as a consequence of Proposition 4.4. Then, $Y \times_W Z \to X \to X$ is also finite étale as a consequence of Proposition 4.8.

G2 Initial object: $\varnothing \to X$ is an initial object.

Finite sums: Let $\{Y_i \to X\}_{i=1}^n$ be a finite set of objects in $\mathbf{FEt}_X$. Then, by Lemma 4.2 we know that the map $\coprod_{i=1}^n Y_i \to X$ is finite étale. Moreover, $\coprod_{i=1}^n Y_i$ is the finite sum of $\{Y_i\}$ in the category of schemes. So, by the universal property of finite sums of schemes, the morphism $\coprod_{i=1}^n Y_i \to X$, together with the inclusion maps $q_i : Y_i \to \coprod_{i=1}^n Y_i \to X$ is the finite sum of the objects $\{Y_i\}$ in $\mathbf{FEt}_X$.

Quotient by a subgroup of automorphisms: We already showed in Proposition 4.13 that quotients by a finite group of automorphisms exist in $\mathbf{FEt}_X$.

G3 Factorization of morphisms: Let $h : Y \to Z$ be a morphism in $\mathbf{FEt}_X$. h is finite étale by Proposition 4.9, and so we can write $Z = Z_0 \amalg Z'$, where $[Y : Z_0] = 0$ and $[Y : Z'] > 0$. As $h^{-1}(Z_0) = \varnothing$, we can factor h as $Y \to Z' \to Z_0 \amalg Z' = Z$. As $[Y : Z'] > 0$, the first map is surjective, and therefore an epimorphism (Proposition 4.10). The second map is an open and closed immersion, so it is a monomorphism by Proposition 4.11.

Monomorphisms are direct summands: This is an immediate consequence of the fact that monomorphisms are open and closed immersions (Proposition 4.11).

To prove axioms $G4 - G6$ we need to define a fundamental functor.

Definition 4.7. A *geometric point* of a scheme X is a morphism $x : \mathrm{Spec}(\Omega) \to X$, where Ω is an algebraically closed field.

It is a basic property of schemes (see Proposition A.8) that a geometric point of a scheme X is equivalent to a point $x \in X$ and an embedding $k(x) \to \Omega$. Therefore, every non-empty scheme (in particular, a connected scheme) admits a geometric point. Now given $Y \to X$ an object in $\mathbf{FEt}_X$ and a geometric point $x : \mathrm{Spec}(\Omega) \to X$, if we base-change to Ω we obtain $Y \times_X \mathrm{Spec}(\Omega)$, which is an object of $\mathbf{FEt}_{\mathrm{Spec}(\Omega)}$. Similarly, a morphism $Y \to Z$ in $\mathbf{FEt}_X$ induces a morphism in $\mathbf{FEt}_{\mathrm{Spec}(\Omega)}$ (as in the proof of Proposition 4.9). This defines a functor $H_x : \mathbf{FEt}_X \to \mathbf{FEt}_{\mathrm{Spec}(\Omega)}$. As Ω is algebraically closed, the absolute Galois group of Ω is trivial, and so the equivalence from Theorem 2.3 (let's denote it by J) is in fact an equivalence between $\mathbf{FEt}_{\mathrm{Spec}(\Omega)}$ and the category of finite sets. $F_x := J \circ H_x$ defines a functor from $\mathbf{FEt}_X$ to **sets**.

Definition 4.8. Let X a connected scheme, $x : \mathrm{Spec}(\Omega) \to X$ a geometric point. We call $F_x : \mathbf{FEt}_X \to \mathbf{FEt}_{\mathrm{Spec}(\Omega)} \to$ **sets** the *fundamental functor of X at x*.

We will now proceed to check that this functor satisfies the axioms G4-G6 of Galois Categories. Note that as J is an equivalence, it will be enough to prove the properties $G4 - G6$ for H_x.

G4 Terminal objects: $X \to X$ is sent to $X \times_X \mathrm{Spec}(\Omega) \to \mathrm{Spec}(\Omega)$, which is indeed the terminal object $\mathrm{Spec}(\Omega) \to \mathrm{Spec}(\Omega)$

Fibred products: Using universal properties of the fibred products, we immediately find the isomorphisms $(Y \times_W Z) \times_X \mathrm{Spec}(\Omega) \cong (Y \times_X \mathrm{Spec}(\Omega)) \times_W (Z \times_X \mathrm{Spec}(\Omega)) \cong (Y \times_X \mathrm{Spec}(\Omega)) \times_{W \times_X \mathrm{Spec}(\Omega)} (Z \times_X \mathrm{Spec}(\Omega))$, which proves that H_x commutes with fibred products.

G5 Initial object: $Y \to X$ is an initial object in $\mathbf{FEt}_X \iff [Y : X] = 0$. Therefore, Proposition 4.4 (iii) implies that $H_x(Y \to X)$ has degree $[Y \times_X \mathrm{Spec}(\Omega) : \mathrm{Spec}(\Omega)] = 0$, and so it is also initial in $\mathbf{FEt}_{\mathrm{Spec}(\Omega)}$.

Sums: $(\coprod_{i=1}^n Y_i) \times_X \mathrm{Spec}(\Omega) \cong \coprod_{i=1}^n (Y_i \times_X \mathrm{Spec}(\Omega))$, and the isomorphism commutes with projections to $\mathrm{Spec}(\Omega)$, so the functor H_x commutes with finite sums.

Epimorphisms: In Proposition 4.10 we showed that $h : Y \to Z$ is an epimorphism in $\mathbf{FEt}_X$ if and only if $[Y : X] \geq 1$. So, using again Proposition 4.4 (iii), the morphism $Y \times_X \mathrm{Spec}(\Omega) \to \mathrm{Spec}(\Omega)$ has also degree $[Y \times_X \mathrm{Spec}(\Omega) : \mathrm{Spec}(\Omega)] \geq 1$ and so it is an epimorphism. This proves that H_x sends epimorphisms to epimorphisms.

Passage to the quotient: The functor H_x commutes with passage to the quotient, as a consequence of Proposition 4.14 taking $Z = \mathrm{Spec}(\Omega)$ in the statement.

G6 As X is connected, $[Y : X]$ is constant for any object $Y \to X$ in $\mathbf{FEt}_X$. Therefore by Proposition 4.4 (iii) we also have that $[Y \times_X \mathrm{Spec}(\Omega) : \mathrm{Spec}(\Omega)]$ is constant. As we know that $J : \mathbf{FEt}_{\mathrm{Spec}(\Omega)} \to$ **sets** sends a separable Ω-algebra of rank n to a set of cardinality n, we have $\#F_x(Y) = [Y : X]$. Now suppose that we have a morphism $h : Y \to Z$ in $\mathbf{FEt}_X$ such that $F_x(h)$ is an isomorphism in **sets**. By the characterization of isomorphisms in the category **sets**, we must have

$$[Y : X] = \#F_x(Y) = \#F_x(Z) = [Z : X]$$

And, in addition, if we write $Z = Z_0 \amalg Z'$ and factor the morphism h as in G3, the fact that $F_x(h)$ is an isomorphism and that F_x commutes with finite sums implies that $F_x(Z_0) = \varnothing \Rightarrow [Z_0 : X] = 0 \Rightarrow Z_0 = \varnothing$ and so h is surjective.

So we can reduce to prove that if $f : Y \to X$ and $g : Z \to X$ are finite étale with $[Y : X] = [Z : X]$, and $h : Y \to Z$ is a surjective morphism between f and g, then h is an isomorphism. Let's start by considering the case with both f and g totally split: In this situation we can choose a covering of X by open sets such that h is trivial above each set of the covering (c.f. Proposition 4.7). Then, h is induced by a morphism $U \times D \to U \times E$, induced at its turn by a map on finite sets $\phi : D \to E$. As $[Y : X] = [Z : X]$, $\#D = \#E$, and as h is surjective, so is ϕ. In conclusion, ϕ is a surjective map between finite sets of the same cardinal, and so ϕ is an isomorphism, and in consequence so is h. In the general case, let's consider a morphism $W \to X$ that is surjective, finite and locally free and that makes both $Y \times_X W \to W$ and $Z \times_X W \to W$ totally split (this can be done as in the proof of Proposition 4.9). Then, using Proposition 4.4(iii) we have that

$$[Y \times_X W : W] = [Y : X] = [Z : X] = [Z \times_X W : W]$$

By the totally split case already dealt with, $Y \times_X W \to Z \times_X W$ is an isomorphism, and so $[Y \times_X W : Z \times_X W] = 1$ by Proposition 4.2. Finally,

$$[Y : Z] = [Y \times_Z (Z \times_X W) : Z \times_X W] = [Y \times_X W : Z \times_X W] = 1$$

Which finishes the proof that $h : Y \to Z$ is an isomorphism.

□

4.5 The étale fundamental group

Definition 4.9 (Étale fundamental group)**.** Let X be a connected scheme, $x : \mathrm{Spec}(\Omega) \to X$ a geometric point and F_x the corresponding fundamental functor at the geometric point. Then, we denote $\pi(X, x) = \mathrm{Aut}(F_x)$, and call it the *étale fundamental group of X at x*.

Consider the category **S** whose objects are pairs (X, x), with X a connected scheme and x a geometric point, with a morphism $(X', x') \to (X, x)$ being a morphism of schemes $f : X' \to X$ such that $f \circ x' = x$. Given a morphism in **S**, the functor $G = - \times_X X' : \mathbf{FEt}_X \to \mathbf{FEt}_{X'}$ satisfies $F_{x'} \circ G \cong F_x$, so by Theorem 2.4 it follows that $\pi(-, -)$ extends to a functor from **S** to the category of profinite groups.

In the case $X = \mathrm{Spec}(K)$, where K is a field, the result of Theorem 4.1 is nothing else than a reformulation of the classical Galois Theory for Fields, apart from the uniqueness statement (c.f. Theorem 2.3). So, in a certain sense, Theorem 4.1 can be seen as a generalization of Galois theory to the category of connected schemes. As well as Galois theory for fields classifies all the finite separable extensions of a field K in terms of the absolute Galois group, Galois theory for schemes classifies all the finite étale coverings of a connected scheme X in terms of the étale fundamental group.

4.6 Examples

In this last section we deal with some examples of interest in number theory. In particular, we will give an explicit description of the fundamental group of a locally noetherian normal integral scheme of dimension one (it should be noted that an integral scheme is irreducible by [3], Proposition II.3.1, and so in particular it is connected and it makes sense to talk about its étale fundamental group). To do this, one needs to completely characterize the finite étale coverings of a scheme of this type. For this purpose we will introduce some definitions and auxiliary results.

Definition 4.10. Let $f : Y \to X$ be a morphism of schemes locally of finite type, and $y = f(x) \in Y$. We say that f is *unramified at* y if $\mathcal{O}_{Y,y}/\mathfrak{m}_x\mathcal{O}_{Y,y}$ is a finite separable field extension of $\mathcal{O}_{X,x}/\mathfrak{m}_x$. We say that f is *unramified* if it is unramified at every point.

Lemma 4.8 (Affine characterization of unramified morphisms)**.** Let A be a ring, B a finitely generated A-algebra, $\mathfrak{q} \in \operatorname{Spec}(B)$. Then, $f : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is unramified at $\mathfrak{q}$ $\iff$ $\mathfrak{p} = f(\mathfrak{q})$ generates the maximal ideal of $B_\mathfrak{q}$ and the residue field $k(\mathfrak{q})$ is a finite separable extension of $k(\mathfrak{p})$.

Proof. The inclusion $\mathcal{O}_{X,x}/\mathfrak{m}_x \to \mathcal{O}_{Y,y}/\mathfrak{m}_x\mathcal{O}_{Y,y}$, when we translate to the affine setting $X = \operatorname{Spec}(A)$, $Y = \operatorname{Spec}(B)$, is identified with the morphism

$$A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \to B_\mathfrak{q}/\mathfrak{p}B_\mathfrak{q}$$

It is indeed clear that if $\mathfrak{p}B_\mathfrak{q} = \mathfrak{q}B_\mathfrak{q} \iff \mathfrak{p}B_\mathfrak{q}$ is maximal in $B_\mathfrak{q}$, which in turn happens if and only if $B_\mathfrak{q}/\mathfrak{p}B_\mathfrak{q}$ is a field. In that case, then the map above is in fact the inclusion $k(\mathfrak{p}) \to k(\mathfrak{q})$, and so if $k(\mathfrak{q})$ is a finite separable field extension of $k(\mathfrak{p})$ if and only if the morphism f is unramified. □

The following lemma shows the relation between the definition we have just introduced and the definition of "unramified" in number theory.

Lemma 4.9. Let A be a Dedekind domain, and let B be the integral closure of A in a finite separable field extension of the field of fractions of A. Let $\mathfrak{q}$ be a maximal ideal of B and $\mathfrak{p} = A \cap \mathfrak{q}$. Then $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is unramified at $\mathfrak{q}$ if and only if the ramification index $e(\mathfrak{q}/\mathfrak{p})$ equals 1 and $B/\mathfrak{q}$ is separable over $A/\mathfrak{p}$.

Proof. Let $\mathfrak{p} = \prod_{i=1}^n \mathfrak{q}_i^{e_i}$, and let $\mathfrak{q} = \mathfrak{q}_1$. Then, $\mathfrak{p}B_\mathfrak{q} = \mathfrak{q}^{e_1}$. Therefore, $\mathfrak{p}B_\mathfrak{q} = \mathfrak{q}B_\mathfrak{q} \iff e(\mathfrak{q}/\mathfrak{p}) = 1$. In that case, we have

$$A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong A/\mathfrak{p} \to B/\mathfrak{q} \cong B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q}$$

and so $B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q}$ is a finite separable field extension of $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ if and only if $A/\mathfrak{p} \to B/\mathfrak{q}$ is a finite separable field extension. This concludes the proof. □

Definition 4.11. A scheme is *normal* if all its local rings are integrally closed domains.

Definition 4.12. If X is an integral scheme, then the local ring of the generic point is a field, called the *function field of* X. See Proposition A.9 for a proof that this is well defined.

Definition 4.13. Let X be a normal integral scheme, let K be its function field and L a finite separable extension of K. Considering $\mathcal{O}_X(U)$ as a subring of K, for every U, define $\mathcal{A}(U)$ as the integral closure of $\mathcal{O}_X(U)$ in L. The assignment $U \mapsto \mathcal{A}(U)$ defines a quasi-coherent sheaf of $\mathcal{O}_X$-algebras, and so it gives rise to an affine morphism $Y = \mathbf{Spec}(\mathcal{A}) \to X$. Under this situation, we say that Y is the *normalization of* X *in* L. We say that X *is unramified in* L if $Y \to X$ is unramified.

Lemma 4.10. Let X be a locally noetherian normal integral scheme with function field K, $K \subset L$ a finite separable field extension. Then,

i) The normalization of X in L is finite over X.

ii) If X has dimension one, then the normalization of X in L, $Y \to X$ is locally free with constant degree $[L : K]$ over X.

Proof. i) By definition, the normalization of X in L is the morphism $f : \mathbf{Spec}(\mathcal{A}) \to X$, and $\mathbf{Spec}(\mathcal{A})$ satisfies the property that for every open affine $X \supset U = \operatorname{Spec}(A)$, $f^{-1}(U) = \operatorname{Spec}(\mathcal{A}(U))$, where $\mathcal{A}(U)$ is the integral closure of A in L. Then, we can reduce the problem to prove that $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is finite if A is noetherian and integrally closed, and B is the integral closure of A in L. By [1], Proposition 5.17, $\exists$ a basis $\{v_1, \dots, v_n\}$ of L over K such that $B \subset \sum_{i=1}^{n} Av_i$. Then, we have that $A \subseteq B \subseteq C = \sum_{i=1}^{n} Av_i$. C is finitely generated as an A-module and A is noetherian, so we are under the hypothesis of [1], Proposition 7.8, and we can conclude that B is finitely generated as an A-algebra. Now using the fact that B is also integral over A, we conclude that it is finitely generated as an A-module.

ii) If X has dimension 1, then for every affine subset of X, $U = \operatorname{Spec}(A)$, A is a Dedekind domain. Recall that a finitely generated module over a Dedekind domain A is projective $\iff$ it is torsionfree (c.f. Proposition A.10). As the notion of degree is local, we can restrict to open affine subsets of X $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$. In this situation, by the result already proven above, B is finitely generated as an A-module, and torsionfree by the fact that A is a domain and the characterization of projective modules over Dedekind domains given in Example 3.1. Then B is a finite projective A-algebra, and therefore it is locally free. Moreover, $[L : K] = [B \otimes_A K : K] = [B : A]$, which concludes the proof. □

Lemma 4.11. Let A be an integrally closed domain, and B a projective separable A-algebra. Then, there are finite separable field extensions $L_1, \dots, L_t$ of K such that there is an isomorphism $B \otimes_A K \cong \prod_{i=1}^{t} L_i$ of K-algebras, and this induces an isomorphism $B \cong \prod_{i=1}^{t} B_i$, where B_i is the integral closure of A in L_i.

Proof. As $B \otimes_A K$ is a separable K-algebra, then by Lemma 2.1 we have an isomorphism $B \otimes_A K \cong \prod_{i=1}^{t} L_i$, for L_i finite separable field extensions of K for every i. As A is a domain, the map $A \to K$ is injective. The fact that B is projective implies in particular that it is flat over A, and so tensoring the map $A \to K$ with B, it yields that $B \to B \otimes_A K$ is injective, and so B can be seen as $B \subset \prod_{i=1}^{n} L_i$. In particular, B is a finitely generated module over A, so every element is integral and therefore the image of B in $\prod_{i=1}^{n} L_i$ is contained in $\prod_{i=1}^{n} B_i$. We want to prove that the equality holds.

Given $x \in \prod_{i=1}^{n} B_i$, and $y \in B$, we have $xy \in \prod_{i=1}^{n} B_i$. We claim that $Tr_{B \otimes_A K/K}(xy) \in A$. Note that we can write $Tr_{B \otimes_A K/K} = \sum_{i=1}^{t} Tr_{L_i/K}$, and therefore it's enough to prove that $Tr_{L_i/K}(z) \in A$, for each $z \in B_i$. Let $\sum_{k=0}^{m} a_k X^k$ (with $a_m = 1$), be the irreducible polynomial of z over L. Let $\{1, z, \dots, z^{n-1}\}$ be a basis of $K(z)$ over K, and let $\{\alpha_1, \dots, \alpha_r\}$ be a basis of L_i over $K(z)$. Then, $\{w_{i,j} = z^i \alpha_j\}_{i,j}$ is a basis of L_i over K. It's clear that the map multiplication by z maps $w_{i,j}$ to $w_{i+1,j}$ if $i < n-1$, and to $-\sum_{k=0}^{m-1} a_k w_{k,j}$ if $i = n-1$. Therefore, $Tr_{L_i/K}(z) = -[L : K(z)]a_{m-1}$. Since A is integrally closed, [1] Proposition 5.15 implies that the coefficients a_k of the irreducible polynomial of z over K lie in A, and this concludes the proof of the claim. The map $B \to A$ sending $y \mapsto Tr(xy)$ is A-linear, so by the definition of separability $\exists x' \in B$ with $Tr_{B \otimes_A K/K}(xy) = Tr_{B/A}(x'y)$ for all $y \in B$. Then, by K-linearity $Tr(xy) = Tr(x'y)$, $\forall y \in B \otimes_A K$. By separability of $B \otimes_A K$ over K, $x = x' \in B$, which concludes the proof. □

Lemma 4.12. Let X be a topological space that can be written as the union of open irreducible subsets. Then X can be written as the disjoint union of open irreducible subsets.

Proof. Let $X = \bigcup_{i \in I} X_i$ with X_i irreducible subsets. Note that we can make a partition of the set I by $I_\alpha \subset I$ such that $\bigcup_{\alpha \in J} I_\alpha = I$ and $I_\alpha \cap I_{\alpha'} = \varnothing$, for each $\alpha, \alpha' \in J$, satisfying $X_i \cap X_j = \varnothing$ if i, j belong to different classes and $X_i \cap X_j \neq \varnothing$ if i, j belong to the same equivalence class. This is possible because the sets X_i are irreducible, so if $X_i \cap X_j \neq \varnothing$ and $X_i \cap X_k \neq \varnothing$ are nonempty open sets in X_i, as X_i is irreducible, $\varnothing \neq (X_i \cap X_j) \cap (X_i \cap X_k) = X_i \cap X_j \cap X_k \subseteq X_j \cap X_k$.

Now define $Y_\alpha = \bigcup_{j \in I_\alpha} X_j$. It is clear that the sets $\{Y_j\}$ are pairwise disjoint and that $X = \coprod_{\alpha \in J} Y_\alpha$. We claim that in addition they are irreducible. Let's observe that given an nonempty open set U of Y_α, we must have $U \cap X_i \neq \varnothing$, for each $i \in I_\alpha$: Otherwise, suppose that $U \cap X_i \neq \varnothing$, and take j such that $U \cap X_j \neq \varnothing$. Then the nonempty open sets $X_j \cap X_i$ and $X_j \cap U$ of X_j have empty intersection, which is a contradiction with the irreducibility of X_j. Then, given two open sets U, V of Y_α, and $i \in I_\alpha$ we have that $U \cap X_i$ and $V \cap X_i$ are nonempty open sets of X_i, so they have nonempty intersection by the irreducibility of X_i. This proves that Y_α is irreducible, which concludes the proof. □

We finally prove the result that characterizes all finite étale coverings of a locally noetherian normal integral scheme of dimension 1. Note that it is enough to characterize connected coverings, as every covering can be written as the sum of connected coverings, by Proposition 2.2 and the fact that $\mathbf{FEt}_X$ is a Galois Category.

Theorem 4.2. *Let X be a locally noetherian normal integral scheme of dimension one, with function field K. Let L be a finite separable field extension of K such that X is unramified in L. Then the normalization of X in L is a connected finite étale covering of X. Moreover, every connected finite étale covering of X arises in this way.*

Proof. We begin with the proof of the last statement: Let $f : Y \to X$ be a connected finite étale covering of X. Let $U = \operatorname{Spec}(A)$ be an open affine subset of X and $f^{-1}(U) = \operatorname{Spec}(B) \subset Y$. We are under the hypothesis of Lemma 4.11, and therefore $\operatorname{Spec}(B) \cong \operatorname{Spec}(B_1) \amalg \cdots \amalg \operatorname{Spec}(B_t)$. Each B_i is integral and therefore $\operatorname{Spec}(B_i)$ is irreducible by [3], Proposition II.3.1, so we can write $f^{-1}(U) = \operatorname{Spec}(B)$ as the disjoint union of open irreducible subsets. Taking the union through all open affine subsets $U \subseteq X$, and using Lemma 4.12, we conclude that we can write Y as the union of open irreducible subsets. As Y is connected, therefore Y itself must be irreducible. On the other side, for every $\operatorname{Spec}(B_i)$ all local rings are domains, which implies that the same statement is true for Y, and so Y is reduced. Putting everything together and using again [3], Proposition II.3.1, we conclude that Y is an integral scheme. Let L be the function field of Y. We claim that $Y \to X$ is the normalization of X in L. Indeed, for every open affine subset of X, $U = \operatorname{Spec}(A)$, $f^{-1}(U) = \operatorname{Spec}(B)$ and Lemma 4.11 together with the fact that Y is irreducible, implies that B is the integral closure of A in the field $B \otimes_A K = L$. Therefore, $Y \to X$ is the normalization of X in L, and X is unramified in L by Theorem A.1. This concludes the proof of the second statement.

To prove the first statement we will use the characterization of Theorem A.1. The morphism $f : Y \to X$ is finite by Lemma 4.10, and it is unramified by hypothesis. Therefore it suffices to prove that $Y \to X$ is a flat morphism. However, using again Lemma 4.10 we know that for every $X \supset U = \operatorname{Spec}(A)$, $f^{-1}(U) = \operatorname{Spec}(B)$ with B a finite projective A-algebra, and so in particular a flat A-module, and this proves that f is flat. □

Lemma 4.13. Let B be a free separable algebra over a field K, $\overline{K}$ an algebraic closure of K and write $B = \prod_{i=1}^{t} B_i$ where each $B_i \subset \overline{K}$ is a finite separable field extension of K. Let $L \subseteq \overline{K}$ be a field extension of K. Then, $B \otimes_K L \cong L^{\dim_K(B)}$ as L-algebras if and only if L contains the normal closure of B_i over K in $\overline{K}$.

Proof. It is enough to prove it for $t = 1$, that is, $B = B_i$ being a finite separable field extension of K. As a consequence of the primitive element theorem, in that situation we can write $B = K[X]/(f)$, for $f \in K[X]$ an irreducible separable polynomial. Then, $B \otimes_K L = L[X]/(f)$. It is trivial that $L[X]/(f)$ splits in simple factors if and only if all the roots of f belong to L, that is, if and only if L contains the normal closure of B over K. □

Definition 4.14. Let K be a field, M a Galois extension of K and B a finite dimensional K-algebra. If $B \otimes_K M \cong M^{\dim_K(B)}$ as M-algebras, we say that M *splits* B.

Lemma 4.14. Let K be a field, and M a Galois extension of K. The category of K-algebras that are split by M is anti-equivalent to Gal(M/K)-**sets**.

Proof. Let B a K-algebra that is split by M, and $\overline{K}$ an algebraic closure of K containing M. Then, $B \otimes_K \overline{K} \cong (B \otimes_K M) \otimes_K \overline{K} \cong \overline{K}^{\dim_K(B)}$. Therefore Lemma 2.1 implies that B is a separable K-algebra, and we can write $B = \prod_{i=1}^{t} B_i$. Using Lemma 4.13, we conclude that M contains the normal closure of B_i in $\overline{K}$ for each i. Therefore, the whole argument of the proof of Theorem 2.3 holds in this situation if we exchange $\overline{K}$ by M, and therefore we can conclude that the category of K-algebras that are split by M is anti-equivalent to Gal(M/K)-**sets**. □

Theorem 4.3. *Let X be a locally noetherian normal integral scheme of dimension one, K its function field, $\overline{K}$ an algebraic closure of K and M the composite of all finite separable field extensions L of K, with $L \subset \overline{K}$ for which X is unramified in L. Then, the fundamental group $\pi(X)$ is isomorphic to the Galois group* Gal(M/K).

Proof. $K \subset M$ is a separable extension, as it is the composition of separable extensions. Moreover, if X is unramified in L, then for every embedding L' of L into $\overline{K}$, X is also unramified in L', which proves that $K \subset M$ is normal and therefore Galois, then it makes sense to talk about Gal(M/K). Now note that the natural morphism Spec$(K) \to X$ induces a functor $G : \mathbf{FEt}_X \to \mathbf{FEt}_{\mathrm{Spec}(K)}$, which sends a morphism $Y \to X$ to $Y \times_X \mathrm{Spec}(K) \to \mathrm{Spec}(K)$. By Theorem 4.2, every connected finite étale covering of X is the normalization of X at some finite separable extension $L \supset K$. Following the reasoning of the proof of Theorem 4.2, it is easily seen that the functor G sends a connected covering $Y \to X$ to Spec$(L) \to$ Spec(K).

This allows us to conclude that the image of the functor G is contained in the set of objects of the form Spec(B), where B is the product of finite separable extensions of K contained in M. By the observation at the beginning of the proof, (and using Lemma 4.13) these are exactly the algebras that are split by M, and so Lemma 4.14 implies that this category is equivalent to Gal(M/K)-**sets**. In conclusion, we have induced a functor $\mathbf{FEt}_X \to \mathrm{Gal}(M/K) - \mathbf{sets}$. Composing it with the equivalence $\mathbf{FEt}_X \to \pi(X) - \mathbf{sets}$, we induce a functor $H : \pi(X)$-**sets** $\to$ Gal(M/K)-**sets**. Then Theorem 2.4 gives rise to a continuous group homomorphism Gal$(M/K) \to \pi(X)$, and it will be enough to prove that this morphism is bijective. For that purpose we will use the characterizations of Proposition 2.10. It is clear that it is surjective, as G sends connected objects to connected objects, and so do the other functors involved because they're equivalences.

Now let's proceed to prove injectivity. Again, as H is the composition of G and equivalences, it will be enough to check that the property holds for G. Let X' be a connected object of $\mathbf{FEt}_{\mathrm{Spec}(K)}$ belonging to the image of G, $X' = \mathrm{Spec}(L)$ for L a finite field separable field extension of K contained in M. If X is ramified in L then we have that the normalization of X in L satisfies the desired property. If this doesn't happen, we can always find finite field extensions $L_1, \dots, L_t$ of K contained in M such that X is unramified in each L_i and such that L is contained in the composite field extension $L_1 L_2 L_t$. Denoting by Y_i the normalization of X in L_i, we have that $Y = Y_1 \times \cdots \times Y_t$ belongs to $\mathbf{FEt}_X$, and $G(Y) = \mathrm{Spec}(L_1 \otimes_K L_2 \otimes_K \cdots \otimes_K L_t)$. The natural epimorphism $L_1 \otimes_K L_2 \otimes_K \cdots \otimes_K L_t \to L_1 L_2 L_t$ sending $x_1 \otimes x_2 \otimes \cdots \otimes x_t \mapsto x_1 x_2 \dots x_t$ shows that there is a monomorphism $\mathrm{Spec}(L_1 L_2 L_t) \to G(Y)$, and as $\mathrm{Spec}(L_1 L_2 L_t)$ is connected, it is a connected component of $G(Y)$. The inclusion $L \subseteq \prod_{i=1}^{t} L_i$ yields a morphism $\mathrm{Spec}(L_1 L_2 L_t) \to \mathrm{Spec}(L)$ in $\mathbf{FEt}_{\mathrm{Spec}(K)}$. Therefore the characterization of Proposition 2.10 is satisfied, and this implies that the map $\mathrm{Gal}(M/K) \to \pi(X)$ induced by H is bijective, and so it is an isomorphism of profinite groups. □

Corollary 4.1. Let's see how the theorem above reads in some particular cases:

- If $X = \mathrm{Spec}(A)$, where A is the ring of integers of a number field K, then A is a Dedekind domain. The field extensions $L \supset K$ such that X is unramified in L are exactly the field extensions such that are unramified at every prime of A. Therefore M is the maximal unramified extension of K, and $\pi(\mathrm{Spec}(A)) = \mathrm{Gal}(M/K)$.

- If $X = \mathrm{Spec}(A[1/a])$, where A is the ring of integers of a number field K, $0 \neq a \in A$, then the primes of $A[1/a]$ are in one to one correspondence with the primes of A that don't divide a. Then M is the maximum field extension of K unramified at all non-zero primes of A that don't divide a, and $\pi(\mathrm{Spec}(A[1/a])) = \mathrm{Gal}(M/K)$.

- As a consequence of Minkowski's theorem ([6], page 130), every extension of $\mathbb{Q}$ ramifies at least in 1 point, and therefore, the maximal unramified extension of $\mathbb{Q}$ is trivial, $M = \mathbb{Q}$. In consequence, the étale fundamental group of $\mathrm{Spec}(\mathbb{Z})$ is trivial, $\pi(\mathrm{Spec}(\mathbb{Z})) = \{1\}$.

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802].

[2] K. Gruenberg. Profinite groups. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 116–127. Thompson, Washington, D.C., 1967.

[3] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[4] Masaki Kashiwara and Pierre Schapira. *Categories and sheaves*, volume 332 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2006.

[5] H.W. Lenstra. Galois theory for schemes, 2008. Avaliable at: http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf.

[6] Hermann Minkowski. *Geometrie der Zahlen*. Bibliotheca Mathematica Teubneriana, Band 40. Johnson Reprint Corp., New York-London, 1968.

[7] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2010.

A. Appendix

A.1 Uniqueness of categorical objects

Lemma A.1. Initial objects and terminal objects are unique up to isomorphism if they exist.

Proof. Let Z_1, Z_2 be terminal objects in $\mathbf{C}$, and $h_1 : Z_1 \to Z_2$, $h_2 : Z_2 \to Z_1$ the unique morphisms. Note that a terminal object in particular has a unique endomorphism, which must be the identity. So this implies that $h_1 \circ h_2 = \mathrm{id}_{Z_1}$ and $h_2 \circ h_1 = \mathrm{id}_{Z_2}$, and so $Z_1 \cong Z_2$. The argument for initial objects is the same one. □

Lemma A.2. The fibred product of two objects X, Y over a third one S, built over morphisms f, g, is unique up to isomorphism if it exists.

Proof. Let $((X \times_S Y)_1, (p_1, p_2))$, $((X \times_S Y)_2, (q_1, q_2))$ be two fibred products of X and Y over S, with morphisms $f : X \to S$, $g : Y \to S$. Then, we have the following commutative diagrams:

$$\begin{tikzcd}
(X \times_S Y)_2 \arrow[dr, dotted, "\theta"] \arrow[drr, bend left, "q_1"] \arrow[ddr, bend right, "q_2"'] & & \\
& (X \times_S Y)_1 \arrow[r, "p_1"] \arrow[d, "p_2"] & X \arrow[d, "f"] \\
& Y \arrow[r, "g"] & S
\end{tikzcd}
\qquad
\begin{tikzcd}
(X \times_S Y)_1 \arrow[dr, dotted, "\chi"] \arrow[drr, bend left, "p_1"] \arrow[ddr, bend right, "p_2"'] & & \\
& (X \times_S Y)_2 \arrow[r, "q_1"] \arrow[d, "q_2"] & X \arrow[d, "f"] \\
& Y \arrow[r, "g"] & S
\end{tikzcd}$$

And so we have that $p_i\theta\chi = p_i$ and $q_i\chi\theta = q_i$. Then, we have the following commutative diagrams

$$\begin{tikzcd}
(X \times_S Y)_1 \arrow[dr, dotted, "a"] \arrow[drr, bend left, "p_1"] \arrow[ddr, bend right, "p_2"'] & & \\
& (X \times_S Y)_1 \arrow[r, "p_1"] \arrow[d, "p_2"] & X \arrow[d, "f"] \\
& Y \arrow[r, "g"] & S
\end{tikzcd}
\qquad
\begin{tikzcd}
(X \times_S Y)_2 \arrow[dr, dotted, "b"] \arrow[drr, bend left, "q_1"] \arrow[ddr, bend right, "q_2"'] & & \\
& (X \times_S Y)_2 \arrow[r, "q_1"] \arrow[d, "q_2"] & X \arrow[d, "f"] \\
& Y \arrow[r, "g"] & S
\end{tikzcd}$$

Using now the fact that $a = \mathrm{id}_{(X \times_S Y)_1}$ and $b = \mathrm{id}_{(X \times_S Y)_2}$ and also $A = \theta\chi$ and $b = \chi\theta$ satisfy the diagram, and the uniqueness of a, b, we finally get $\theta\chi = \mathrm{id}_{(X \times_S Y)_1}$ and $\chi\theta = \mathrm{id}_{(X \times_S Y)_2}$, so $(X \times_S Y)_1 \cong (X \times_S Y)_2$ □

Lemma A.3. The sum of a collection of objects $(X_i)_{i \in I}$ is unique up to isomorphism if it exists.

Proof. Let $(X, (q_i)_{i \in I})$ and $(Y, (p_i)_{i \in I})$ be two sums of the objects $(X_i)_{i \in I}$. Then, by the universal property of the sum, $\exists! f : X \to Y$ satisfying $p_i = fq_i$ and $\exists! g : Y \to X$ such that $q_i = gp_i$. Therefore we have $q_i = gfq_i$, $p_i = fgp_i$. On the other hand, considering the maps $q_i : X_i \to X$, we have that $\exists! mapa : X \to X$ such that $q_i = aq_i \forall i$. But as id satisfies that property, then $a = \mathrm{id}$. This proves that $gf = \mathrm{id}_X$. The same argument on Y proves that $fg = \mathrm{id}_Y$, and so $X \cong Y$. □

Lemma A.4. Given $X \in Ob(\mathbf{C})$ and $G \subset \mathrm{Aut}_{\mathbf{C}}(A)$, the quotient of X by G is unique up to isomorphism.

Proof. Let $((X/G)_1, p_1)$ and $((X/G)_2, p_2)$ be two quotients of X by G. The applications p_i satisfy $p_i\sigma = p_i, \forall \sigma \in G$, so we have the following commutative diagrams:

$$\begin{tikzcd}
X \arrow[r, "p_1"] \arrow[d, "p_2"] & (X/G)_1 \arrow[dl, dotted, "g"] \\
(X/G)_2 &
\end{tikzcd}
\qquad
\begin{tikzcd}
X \arrow[r, "p_2"] \arrow[d, "p_1"] & (X/G)_2 \arrow[dl, dotted, "h"] \\
(X/G)_1 &
\end{tikzcd}$$

So we have that $gp_1 = p_2$ and $hp_2 = p_1$, so $ghp_2 = p_2$ and $hgp_1 = p_1$. By uniqueness, we must have $gh = \mathrm{id}_{(X/G)_2}$ and $hg = \mathrm{id}_{(X/G)_1}$, so $(X/G)_1 \cong (X/G)_2$. □

Lemma A.5. The equalizer of two morphisms $f, g : X \to Y$ is unique up to isomorphism if it exists.

Proof. Suppose that we have (E_1, θ_1), (E_2, θ_2) two equalizers of f, g. We have that $f\theta_i = g\theta_i$, so there are unique maps $h_1 : E_1 \to E_2$, $h_2 : E_2 \to E_1$ satisfying $\theta_2 h_1 = \theta_1$ and $\theta_1 h_2 = \theta_2$. The following diagrams illustrate the situation.

$$\begin{tikzcd}
E_1 \arrow[r, "\theta_1"] \arrow[dr, dotted, "h_1"] & X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \\
& E_2 \arrow[u, "\theta_2"] &
\end{tikzcd}
\qquad
\begin{tikzcd}
E_2 \arrow[r, "\theta_2"] \arrow[dr, dotted, "h_2"] & X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \\
& E_1 \arrow[u, "\theta_1"] &
\end{tikzcd}$$

Then we have $\theta_1 h_2 h_1 = \theta_1$ and $\theta_2 h_1 h_2 = \theta_2$. Then consider the following diagram

$$\begin{tikzcd}
E_1 \arrow[r, "\theta_1"] \arrow[dr, dotted, "a"] & X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \\
& E_1 \arrow[u, "\theta_1"] &
\end{tikzcd}$$

We have that both $a = h_2 h_1$ and $a = \mathrm{id}_{E_1}$ make the diagram commutative, so by uniqueness, $h_2 h_1 = \mathrm{id}_{E_1}$. The same argument shows that $h_1 h_2 = \mathrm{id}_{E_2}$, and so $E_1 \cong E_2$. □

A.2 Algebra and scheme theory

Proposition A.1. ([1], Exercise 1.21) Let $\phi : A \to B$ be a ring homomorphism. Let $X = \mathrm{Spec}(A)$ and $Y = \mathrm{Spec}(B)$. If $\mathfrak{q} \in Y$, then $\phi^{-1}(\mathfrak{q})$ is a prime ideal of A, i.e., a point of X. Hence ϕ induces a mapping $\phi^* : Y \to X$. Then,

(i) If $\mathfrak{b}$ is an ideal of B, then $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{b}^c)$.

(ii) If ϕ is injective, then $\phi^*(Y)$ is dense in X. More precisely, $\phi^*(Y)$ is dense in $X \iff Ker(\phi) \subseteq \mathfrak{R}$.

Proof. (i) $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{a})$, for some ideal $\mathfrak{a}$ yet to determine. We observe that $x \in \phi^*(V(\mathfrak{b})) \iff \exists y \in \mathrm{Spec}(B)$ such that $\mathfrak{p}_y \supseteq \mathfrak{b}$ and $\mathfrak{p}_x = \mathfrak{p}_y^c$. Then, it's clear that $\mathfrak{a} \subseteq \mathfrak{p}^c$, $\forall \mathfrak{p} \supseteq \mathfrak{b}$, which implies that $\mathfrak{a} \subseteq \bigcap_{\mathfrak{p}\supseteq\mathfrak{b}} \mathfrak{p}^c$. As the closure is the smallest closed subset containing $\phi^*(V(\mathfrak{b}))$, we have the equality

$$\overline{\phi^*(V(\mathfrak{b}))} = V\left(\bigcap_{\mathfrak{q}\supseteq\mathfrak{b}} \mathfrak{q}^c\right)$$

Therefore,

$$V\left(\bigcap_{\mathfrak{q}\supseteq\mathfrak{b}} \mathfrak{q}^c\right) = V\left(\left(\bigcap_{\mathfrak{q}\supseteq\mathfrak{b}} \mathfrak{q}\right)^c\right) = V(r(\mathfrak{b})^c) = V(r(\mathfrak{b}^c)) = V(\mathfrak{b}^c)$$

(ii) $\phi^*(Y)$ is dense in $X \iff \overline{\phi^*(Y)} = X$. We also know that

$$\overline{\phi^*(Y)} = \overline{\phi^*(V((0)))} = V((0)^c) = V(\ker(\phi))$$

Therefore, we only have to show that $V(\ker(\phi)) = X \iff \ker(\phi) \subseteq \mathfrak{R}$. That is true because $V(\ker(\phi)) = X \iff \mathfrak{p} \supseteq \ker(\phi)\ \forall \mathfrak{p}$ prime $\iff \bigcap_{\mathfrak{p}\text{ prime}} \mathfrak{p} \supseteq \ker(\phi) \iff \ker(\phi) \subseteq \mathfrak{R}$.

□

Proposition A.2. ([1], Exercise 2.11) Let A be a ring. Then, $A^n \cong A^m$ as A-modules $\iff n = m$.

Proof. Let $\mathfrak{m}$ be a maximal ideal of A, $k = A/\mathfrak{m}$ and let $\phi : A^m \to A^n$ be an isomorphism. As tensor product commutes with direct sums, $A/\mathfrak{m} \otimes A^m \cong \bigoplus_{i=1}^m A/\mathfrak{m} \otimes A \cong k^m$.

In conclusion $A/\mathfrak{m} \otimes A^m$ is a m-dimensional k-vector space and similarly, $A/\mathfrak{m} \otimes A^n$ is a n-dimensional k-vector space. The isomorphism between A^m and A^n is equivalent to the exactness of the sequence $0 \to A^m \to A^n \to 0$. Then, by 2.18, tensoring the sequence preserves the exactness, and therefore $0 \to A/\mathfrak{m} \otimes A^m \to A/\mathfrak{m} \otimes A^n \to 0$ is exact, which implies that $1 \otimes \phi : A/\mathfrak{m} \otimes A^m \to A/\mathfrak{m} \otimes A^n$ is an isomorphism of vector spaces. So the dimensions of the spaces must be the same $\Rightarrow n = m$. □

Proposition A.3. ([3], Chapter II Exercise 5.17 (a)) If $f : Y \to X$ is affine, $\forall U = \mathrm{Spec}(A)$ open affine subset of X, $f^{-1}(U) = V = \mathrm{Spec}(B)$ is affine.

Proof. Let's observe first that if $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is a morphism of schemes, then $\forall f \in A$, the restriction of this morphism to $D(f)$ corresponds to the morphism of schemes $\mathrm{Spec}(B_f) \to \mathrm{Spec}(A_f)$. If we apply this observation to an open affine covernig of X $\{U_i = \mathrm{Spec}(A_i)\}$ such that $f^{-1}(U_i) = \mathrm{Spec}(B_i)$, and taking into account that the sets $D_i(f_j) = \mathrm{Spec}((A_i)_{f_j})$ form a base of the topology of X, we conclude that every affine set $U = \mathrm{Spec}(A) \subset X$ can be covered by open affine sets with affine antiimage, and therefore, we can reduce to prove the case in which X is affine.

Now let $X = \mathrm{Spec}(A)$ and U_i as before. For each point $x \in X$, there exists an element $f \in A$ such that $x \in D(f) \subset U_i$ for a certain i. Then, if we denote $\overline{f}$ for the image of f in A_i, we have $D(f) \cong \mathrm{Spec}((A_i)_{\overline{f}})$, and so its antiimage is affine, $f^{-1}(D(f)) = \mathrm{Spec}((B_i)_{\overline{f}}$. The morphism $f : Y \to \mathrm{Spec}(A)$ corresponds uniquely to a map $\varphi : A \to \Gamma(Y, \mathcal{O}_Y)$. If we consider the restriction of f to $f^{-1}(D(f))$, we have that $P \in g^{-1}(D(f)) \iff g(P) \in D(f) \iff \varphi(f)_{\mathfrak{p}} \notin \mathfrak{m}_P \iff P \in Y_{\varphi(f)}$. Therefore we have proven that $Y_{\varphi(f)}$ is affine.

By compactness, we can always take a finite number of elements f of this type that generate $(1) \in A$, and this implies that their images by φ also generate $1 \in \Gamma(Y, \mathcal{O}_Y)$, which is enough to conclude that Y is affine. □

Proposition A.4. ([3], Chapter II Exercise 3.4) If $f : Y \to X$ is finite, $\forall U = \mathrm{Spec}(A)$ open affine subset of X, $f^{-1}(U) = V = \mathrm{Spec}(B)$ is a finite A-algebra.

Proof. A finite morphism is in particular affine. Therefore, by the result above, for every $U = \mathrm{Spec}(A) \subseteq X$, we will have $f^{-1}(U) = \mathrm{Spec}(B)$. Now we only have to prove that B is a finitely generated A-module, but we know that $\exists (f_i)_{i\in I}$, $f_i \in A$ such that $(f_i) = (1)$ and U can be covered by the sets $\{D(f_i)\}$, with $f^{-1}(D(f_i)) = \mathrm{Spec}(C_i)$, and C_i is a finitely generated A_{f_i}-module. Then Lemma 3.4 (ii) concludes the proof. □

Proposition A.5. ([3], Chapter II Exercise 2.19) Let A be a ring. Then, the following conditions are equivalent:

i) $\mathrm{Spec}(A)$ is disconnected;

ii) there exist nonzero elements $e_1, e_2 \in A$ such that $e_1e_2 = 0$, $e_1^2 = e_1$, $e_2^2 = e_2$, $e_1 + e_2 = 1$ (these elements are called orthogonal idempotents);

iii) A is isomorphic to a direct product $A_1 \times A_2$ of two nonzero rings.

Proof. $\boxed{(iii) \Rightarrow (ii)}$ Let $\phi : A_1 \times A_2 \to A$ be an isomorphism. Then consider $e_1 := \phi((1,0))$ and $e_2 := \phi((0,1))$. Then $e_1^2 = \phi((1,0))^2 = \phi((1,0)^2) = \phi((1,0)) = e_1$ and analogoulsy with e_2, so $e_i^2 = e_i$. $e_1e_2 = \phi((1,0))\phi((0,1)) = \phi((1,0)(0,1)) = \phi(0) = 0$ and $e_1 + e_2 = \phi((1,0)) + \phi((0,1)) = \phi((1,0) + (0,1)) = \phi(1) = 1$.

$\boxed{(ii) \Rightarrow (i)}$ $V(e_i)$ are closed sets. The ideal generated by e_1, e_2 is the whole ring, so $\varnothing = V((e_1, e_2)) = V(e_1 \cup e_2) = V(e_1) \cap V(e_2)$. Moreover $(e_1)(e_2) = (e_1e_2) = 0$, so $V(e_1) \cup V(e_2) = V((e_1)(e_2)) = V(0) = \mathrm{Spec}(A)$, and therefore $\mathrm{Spec}(A)$ is disconnected.

$\boxed{(i) \Rightarrow (iii)}$ First let's observe that it is enough to find two ideals $\mathfrak{a}_1, \mathfrak{a}_2$ such that A is the direct sum of these ideals, i.e. $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, $\mathfrak{a}_1 \cap \mathfrak{a}_2 = 0$ because $A_1 \times A_2 = A_1 \oplus A_2$ and the application $\psi : A \to A/\mathfrak{a}_1 \times A/\mathfrak{a}_2$, $x \mapsto (x_1, x_2)$, where x_i is the class of x in $A/\mathfrak{a}_i$ is bijective. Indeed, $\psi(a) = (0,0) \Rightarrow a \in \mathfrak{a}_1 \cap \mathfrak{a}_2 = 0$, so ψ is injective. In addiction each $y_1 \in A/\mathfrak{a}_1$ has a representant $x_1 \in \mathfrak{a}_2$, and each $y_2 \in A/\mathfrak{a}_2$ has a representant $x_2 \in \mathfrak{a}_1$, so $\psi(x_1 + x_2) = (y_1, y_2)$ and ψ is bijective.

So now let's proceed to find these ideals. As $\mathrm{Spec}(A)$ is disconnected, $\exists \mathfrak{a}_1, \mathfrak{a}_2 \neq A$ such that $\mathrm{Spec}(A) = V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$, which implies that $\mathfrak{a}_1\mathfrak{a}_2$ is included in the nilradical of A; It also happens that $V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2) = \varnothing$, which implies that $\mathfrak{a}_1 + \mathfrak{a}_2 = (1)$. These ideals are still not what we are looking for because their intersection is not necessarily 0. But as the sum of the two ideals is the whole ring, $\exists a_i \in \mathfrak{a}_i$ such that $a_1 + a_2 = 1$. $a_1a_2 \in \mathfrak{a}_1\mathfrak{a}_2$ and therefore it is a nilpotent element. Let n such that $(a_1a_2)^n = 0$. Then $1 = 1^n = (a_1 + a_2)^n = a_1^n + a_2^n + b$, where b is a nilpotent element, because it is the sum of elements $a_1^k a_2^m$, with $m, k \geq 1$, which belong to $\mathfrak{a}_1\mathfrak{a}_2$, and therefore are nilpotents. Now $a_1^n + a_2^n = 1 - b$, and therefore it's a unit, as it is the sum of a unit and a nilpotent element. In consequence, we have $(a_1^n) + (a_2^n) = (1)$ and the intersection of these two ideals is equal to their product, as they're coprime (Proposition 1.10 of [1]). So we have that $(a_1^n) \cap (a_2^n) = (a_1^n)(a_2^n) = ((a_1a_2)^n) = 0$. Therefore $A = (a_1^n) \oplus (a_2^n)$ and so $A \cong A/(a_1^n) \times A/(a_2^n)$. These rings are both nonzero because $\mathfrak{a}_i \neq A$ (as the close sets $V(\mathfrak{a}_i)$ are not the whole ring, otherwise they wouldn't be a disconnection of $\mathrm{Spec}(A)$). □

Proposition A.6. ([1], Exercise 1.12) Let A be a local ring. Let $x \in A$ such that $x^2 = x$. Then, either $x = 0$ or $x = 1$.

Proof. $x^2 = x \Rightarrow x(x-1) = 0$, so $x(1-x)$ belongs to the maximal ideal, which is equal to the Jacobsol radical because the ring A is local. Then either x or $1 - x$ belongs to the Jacobson radical. In the first case, this implies that $1-x$ is a unit and in the second case, that x is a unit. On conclusion, multiplying the expression $x(1-x)=0$ by the inverse of the unit, it yields that either x or $1-x$ is 0, so $x=0$ or $x=1$. □

Proposition A.7. ([3], Chapter II Exercise 5.17 (b)-(d))

i) Let X be a scheme, and $\mathcal{A}$ a quasi-coherent sheaf of $\mathcal{O}_X$-algebras. Then, $\exists! Y$ and an affine morphism of schemes $f : Y \to X$ such that $\forall V \subseteq Y$, $f^{-1}(V) \cong \operatorname{Spec}(\mathcal{A}(V))$ and for every inclusion $U \subseteq V$, $f^{-1}(U) \subseteq f^{-1}(V)$ corresponds to the restriction $\mathcal{A}(V) \to \mathcal{A}(V)$. We denote $Y = \mathbf{Spec}(\mathcal{A})$.

ii) For every affine morphism of schemes $f : Y \to X$, then $f_*\mathcal{O}_Y$ is a quasi-coherent sheaf of $\mathcal{O}_Y$-algebras, and $Y \cong \mathbf{Spec}(\mathcal{A})$.

iii) Given a scheme X, the category of affine morphisms $\mathbf{Aff}_X$ and the category of quasi-coherent sheafs of $\mathcal{O}_X$-algebras are anti-equivalent.

Proof. i) For each open set $U \subseteq X$ we have a morphism of rings $\mathcal{O}_X(V) \to \mathcal{A}(V)$. Let's choose an open affine covering of X, $\{U_i = \operatorname{Spec}(A_i)\}$. Then $\mathcal{A}(U_i)$ is an A_i-algebra, so we have a morphism $\mathcal{O}_X(U_i) = A_i \to \mathcal{A}(U_i)$, which induces a morphism $\operatorname{Spec}(\mathcal{A}(V_i)) \to \operatorname{Spec}(A_i)$. For each $i \neq j$, there is an open affine subset $U_{ij} = \operatorname{Spec}(\mathcal{A}(V_i \cap V_j)) \subseteq \operatorname{Spec}(\mathcal{A}(V_i))$ corresponding to the natural restriction morphism $\mathcal{A}(V_i) \to \mathcal{A}(V_i \cap V_j)$. There are also isomorphisms of schemes $U_{ij} \cong U_{ji}$. Therefore we can glue all the schemes $\operatorname{Spec}(\mathcal{A}(V_i))$ and this yields a scheme Y satisfying the desired properties.

ii) As f is an affine morphism, there is an open cover of X by open affine subsets $U_i = \operatorname{Spec}(A_i)$ such that $f^{-1}(U_i) = \operatorname{Spec}(B_i)$. Therefore, we have $\mathcal{A}(U_i) = B_i$, which is an A_i-algebra (and therefore an A_i-module). This proves that $\mathcal{A}$ is a quasi-coherent sheaf of $\mathcal{O}_Y$-algebras.

iii) The previous results (i), (ii) define an assignment **Spec** from the category of quasi-coherent sheaves of $\mathcal{O}_X$-algebras to the category of affine morphisms with target X ($\mathbf{Aff}_X$), and $-_*\mathcal{O}_X$ from the category of affine morphisms to quasi-coherent sheaves. It is immediately seen from the definition of thie correspondence that it is bijective, so we just have to check that the assignment is functorial, i.e. that it extends to morphisms of these categories. Indeed, given objects $f, g \in \mathbf{Aff}_X$, and a morphism h from f to g:

$$\begin{tikzcd} Y \arrow[r, "f"] \arrow[d, "h"] & X \\ Z \arrow[ru, "g"] & \end{tikzcd}$$

We know that $f_*\mathcal{O}_X$ and $g_*\mathcal{O}_X$ are quasi-coherent sheafes of $\mathcal{O}_X$-algebras.

Therefore, the morphism $h^{\#} : \mathcal{O}_Z \to h_*\mathcal{O}_Y$ (which is a morphism of rings $\mathcal{O}_Z(V) \to \mathcal{O}_Y(h^{-1}(V))$ for every V open set of Z), when it is restricted to open sets of the form $V = g^{-1}(U)$ yields a morphism of quasi-coherent sheaves of $\mathcal{O}_X$-algebras, $g_*\mathcal{O}_X \to f_*\mathcal{O}_X$.

Reciprocally, a morphism of quasi-coherent sheaves of $\mathcal{O}_X$-algebras $\mathcal{A} \to \mathcal{B}$ corresponds to morphisms of $\mathcal{O}_X(U)$-algebras for every open set $U \subseteq X$.

$$\begin{tikzcd} \mathcal{A}(U) \arrow[r] \arrow[d] & \mathcal{B}(U) \\ \mathcal{O}_X(U) \arrow[ru] & \end{tikzcd}$$

Then this morphisms induce affine morphisms $\operatorname{Spec}(\mathcal{B}(U)) \to \operatorname{Spec}(\mathcal{A}(U))$, which can be glued to form a morphism $\mathbf{Spec}(\mathcal{B}) \to \mathbf{Spec}(\mathcal{A})$.

□

Proposition A.8. ([3], Chapter II Exercise 2.7) Let X be a scheme. For any $x \in X$, let $\mathcal{O}_X$ be the local ring at x and $\mathfrak{m}_x$ its maximal ideal. We define the residual field of x on X to be the field $k(x) = \mathcal{O}_X/\mathfrak{m}_x$.

Now let K be any field. Giving a morphism of $\text{Spec}(K)$ to X is equivalent to give a point $x \in X$ and an inclusion map $k(x) \to K$.

Proof. Let $P \in \text{Spec}(K)$ be the only point of this topological space. Given a morphism of schemes, $(f, f^{\#}) : (\text{Spec}(K), \mathcal{O}_{\text{Spec}(K)}) \to (X, \mathcal{O}_X)$, f is completely determined by a point $x \in X$, the image of the only point $P \in \text{Spec}(K)$. In addition, $f^{\#}$ induces a morphism on the stalks $f_P^{\#} : \mathcal{O}_{X,x} \to K$. It is a local morphism because $(f, f^{\#})$ is a morphism of locally ringed spaces, and so $\ker(f_P^{\#}) = (f_P^{\#})^{-1}(0) = \mathfrak{m}_x$ and therefore we can induce an injective morphism $k(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x \to k$. Reciprocally, given an injection $k(x) \to K$ we can induce a unique local morphism $\mathcal{O}_{X,x} \to K$ sending an element to its class in $k(x)$ and then applying φ. We will see now that any morphism $f^{\#}$ on the structure sheafs it totally determined by the induced application on the stalk at P.

Indeed, given an open set $U \subseteq X$, if $x \notin U$ then $f^{-1}(U) = \varnothing$, so the only possible application $\mathcal{O}_X(U) \to \mathcal{O}_{\text{Spec}(K)}(f^{-1}(U))$ is the zero application. Now let's observe that if $x \in U, V$ and $V \subseteq U$, then the restriction morphisms from $f^{-1}(U)$ to $f^{-1}(V)$ is the identity, and therefore $f^{\#}(U)(s) = f^{\#}(U)(s)|_{f^{-1}(V)} = f^{\#}(V)(s|_V)$. That means that two elements $s, t \in \mathcal{O}_X(U)$ have the same image by $f^{\#}(U)$ if and only if they're equal in a neighbourhood of x. In conclusion, the image of an element s by $f^{\#}(U)$ is equal to the image of its stalk at x by the application $f_P^{\#}$.

In conclusion, a morphism of schemes $(f, f^{\#}) : (\text{Spec}(K), \mathcal{O}_{\text{Spec}(K)}) \to (X, \mathcal{O}_X)$ is completely determined by a point $x \in X$ and an injection $k(x) \to K$. □

Proposition A.9. ([3], Chapter II Exercises 2.9 and 3.6)

i) If X is a topological space, and Z an irreducible closed subset of X, a *generic point for Z* is a point ζ such that $Z = \overline{\{\zeta\}}$. If X is a scheme, every (nonempty) closed subset has a unique generic point.

ii) Let X be an integral scheme. Then, the local ring $\mathcal{O}_\zeta$ of the generic point ζ of X is a field, called the *field of functions of X*. Moreover, for every open affine subset $U = \text{Spec}(A) \subseteq X$, $\mathcal{O}_\zeta \cong K$, where K is the field of fractions of A.

Proof. i) Foreach $P \in Z$, let's consider V_P the open neighbourhood of P such that $(V_P, \mathcal{O}_X|_{V_P})$ is isomorphic to the spectrum of a given ring. Let's fix $P \in Z$ and let A such that $(V_P, \mathcal{O}_X|_{V_P}) \cong (\text{Spec}(A), \mathcal{O}_{\text{Spec}(A)})$. Let f be the homeomorphism $f : V_P \to \text{Spec}(A)$.

Let's observe that $Z \cap V_P$ is irreducible (as an open set of $Z \cap V_P$ is of the form $U \cap Z \cap V_P$ and then $(U_1 \cap Z \cap V_P) \cap (U_2 \cap Z \cap V_P) = (Z \cap V_P) \cap (Z \cap U_1) \cap (Z \cap U_2)$ which is non empty because it's the intersection of nonempty open sets of Z, which is irreducible.

As f is an homeomorphism, then $f(Z \cap V_P)$ is irreducible and closed (as a subset of $\text{Spec}(A)$). As it is closed, $\exists \mathfrak{a}$ ideal of A such that $f(Z \cap V_P) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$. Now let $fg \in r(\mathfrak{a}) \Rightarrow fg \in \mathfrak{q}\ \forall \mathfrak{q} \in V(\mathfrak{a}) \Rightarrow D(fg) \cap V(\mathfrak{a}) = \varnothing$. As $D(fg) = D(f) \cap D(g)$ (Atiyah-MacDonald, exercise 1.17), then $(D(f) \cap V(\mathfrak{a})) \cap (D(g) \cap V(\mathfrak{a})) = \varnothing$. By irreducibility of $V(\mathfrak{a})$, either $D(f) \cap V(\mathfrak{a})$ or $D(g) \cap V(\mathfrak{a})$ must be empty, so either f or g belong to $\mathfrak{q}$, $\forall \mathfrak{q} \in V(\mathfrak{a})$. In conclusion, $r(\mathfrak{a})$ is a prime ideal, that we will name $\mathfrak{p}$, and $f(Z \cap V_P) = V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$, and $\mathfrak{p}$ is the only point of $\text{Spec}(A)$ with this property. Then, $f^{-1}(\mathfrak{p}) = Q_P \in V_P \cap Z$, and as the closure of image is the image of the closure under an homeomorphism, then $\overline{\{Q_P\}} = Z \cap V_P$, where the closure here is the closure in V_P. Then, the closure of Q_P in Z is $\overline{\{Q_P\}} = Z \cap \overline{V_P}$.

Now note that $Z \setminus (Z \cap \overline{V_P})$ and $Z \cap V_P$ are open sets of Z, and their intersection is empty. As Z is irreducible, one of them must be empty. $Z \cap V_P$ is not empty, as P belongs to this subset, so we must have $Z \setminus (Z \cap \overline{V_P}) = \varnothing \Rightarrow Z \cap \overline{V_P} = Z$. So, in conclusion, $\overline{\{Q_P\}} = Z$ and we have proved the existence of a generic point of Z. Now let's prove the uniqueness. Note that the point Q_P is unique with this property in $V_P \cap Z$ (as $\mathfrak{p}$ was unique, as we already observed), but we could have a different point Q_P for each open set V_P. However, as $\overline{\{Q_P\}} = Z$, $\forall P' \in Z$ and $\forall U$ open neighbourhood of P', $Q \in U$. In particular, taking $U = V_{P'}$ we have that $Q_P \in V_{P'}$, and therefore $Q_P = Q_{P'}$ (via the composition of homeomorphisms from V_P and $V_{P'}$ to the corresponding ring spectrums) and so the generic point is unique, $\exists \zeta = Q_P \; \forall P$ such that $Z = \overline{\{\zeta\}}$.

ii) An integral scheme is irreducible ([3], Proposition II.3.1), and so it has a generic point ζ. The local ring of the generic point $\mathcal{O}_\zeta$ is the set of equivalence classes of pairs (U, x), with $x \in \Gamma(X, U)$, and $\zeta \in U$. It is clear that every open affine subscheme contains ζ, as $\overline{\{\zeta\}} = X$. Moreover, the closure of ζ in an open subscheme is the whole open set, so ζ corresponds to the prime ideal (0) when the scheme is affine. If $U = \mathrm{Spec}(A)$, the local ring is then the localization of A in (0), which is indeed the field of fractions of K.

□

Proposition A.10. ([1], Exercise 9.5) Let M be a finitely generated module over a Dedekind domain A. Then, M is flat $\iff$ M is torsionfree.

Proof. The inverse implication is always true, let's prove the direct one. Let's remind that being torsionfree is a local property: M is torsionfree if and only if $M_\mathfrak{m}$ is torsionfree for every maximal ideal $\mathfrak{m}$. Let $\{x_1, \dots x_n\}$ be a minimal set of generators of $M_\mathfrak{m}$ over $A_\mathfrak{m}$, which is a DVR. Then, we can consider the map $A_\mathfrak{m}^n \to M_\mathfrak{m}$, $(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i x_i$, which is surjective. As $A_\mathfrak{m}$ is a DVR, every nonzero element can be written as $a = bm^k$, with $b \in A^*$ and $m \in (\mathfrak{m})$. We will prove that the mapping defined is also injective: Consider $\sum_{i=1}^n a_i x_i = 0$ and write $a_i = b_i m^{k_i}$. Assume without loss of generality that $\min\{k_i\} = k_1$. We have

$$\sum_{i=1}^n b_i m^{k_i} x_i = 0 \Rightarrow m^{k_1} \sum_{i=1}^n b_i m^{k_i - k_1} x_i = 0 \Rightarrow x_1 = \frac{-1}{b_1} \sum_{i=2}^n b_i m^{k_i - k_1} x_i$$

This contradicts that the system of generators is minimal. In consequence, we must have $a_i = 0 \forall i$, and the map is injective. In conclusion, $M_\mathfrak{m}$ is a free module, so M is projective and therefore flat. □

A.3 Alternative characterization of finite étale morphisms

Definition A.1. A morphism of schemes $f : Y \to X$ is *flat* if for every $y \in Y$ the induced morphism on stalks $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is flat.

Proposition A.11. Let $f : A \to B$ be a ring homomorphism. Then the following are equivalent:

i) f is flat
ii) For every prime ideal $\mathfrak{q}$ of B, and $\mathfrak{p} = f^{-1}(\mathfrak{q})$, the induced map $A_\mathfrak{p} \to B_\mathfrak{q}$ is flat.
iii) The induced morphism $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is flat.
iv) For every maximal ideal $\mathfrak{q}$ of B, and $\mathfrak{p} = f^{-1}(\mathfrak{q})$, the induced map $A_\mathfrak{p} \to B_\mathfrak{q}$ is flat.

Proof. $\boxed{(i) \Rightarrow (ii)}$ Let $S = A \setminus \mathfrak{p}$. If f is flat, then so is the induced morphism $A_\mathfrak{p} = S^{-1}A \to S^{-1}B$, by [1], 2.20. Moreover by [1], Proposition 3.6, $S^{-1}B \to B_\mathfrak{q}$ is flat. Therefore given an exact sequence of $A_\mathfrak{p}$ modules, tensoring with $S^{-1}B$ yields an exact sequence of $S^{-1}B$ modules. If we tensor then again by $B_\mathfrak{q}$ the sequence is still exact, so, in conclusion, $A_\mathfrak{p} \to B_\mathfrak{q}$ is flat.

$\boxed{(ii) \Rightarrow (iii)}$ Is true by definition of flat morphism of schemes.

$\boxed{(iii) \Rightarrow (iv)}$ Is true by definition of flat morphism of schemes.

$\boxed{(iv) \Rightarrow (i)}$ By [1] 2.19, it is enough to show that for every injective A-linear map $M \to N$, the induced map $M \otimes_A B \to N \otimes_A B$ is injective. If $M \to N$ is injective, then for any maximal ideal $\mathfrak{q}$ of B the map $M \otimes A_\mathfrak{p} \to N \otimes_A A_\mathfrak{p}$ is injective, by flatness of $A \to A_\mathfrak{p}$ (we are using here again [1], 2.20). Then, by hypothesis $M \otimes_A B_\mathfrak{q} \to N \otimes_A B_\mathfrak{q}$ is injective. As $B \to B_\mathfrak{q}$ is flat, then the kernel K of the map $M \otimes_A B \to N \otimes_A B$ satisfies $K \otimes B_\mathfrak{q} = 0$. As this holds for every maximal ideal, then $K = 0$ by [1], Proposition 3.8. □

We immediately have the following corollary, which is the application of the proposition to the case of non affine schemes.

Corollary A.1. Let $f : Y \to X$ be a morphism of schemes. Then the following statements are equivalent.

i) f is flat

ii) For any pair of open affine subsets $V = \mathrm{Spec}(B) \subset Y$, $U = \mathrm{Spec}(A) \subset X$ with $f(V) \subset U$, the induced ring homomorphism $A \to B$ is flat.

iii) There is a covering of Y by open affine subsets $V_i = \mathrm{Spec}(B_i)$ such that foreach i there is an open affine subset $U_i = \mathrm{Spec}(A_i) \subset X$ with $f(V_i) \subset U_i$ for which the induced ring homomorphism $A_i \to B_i$ is flat.

iv) For every closed point $y \in Y$, the induced ring homomorphism $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is flat.

Definition A.2. A morphism of schemes $f : Y \to X$ is called *finitely presented* if it exists an open affine covering of X, $\{U_i = \mathrm{Spec}(A_i)\}$ such that for each i the open subscheme $f^{-1}(U_i)$ is affine, $f^{-1}(U_i) = \mathrm{Spec}(B_i)$ and B_i is an A_i-algebra that is finitely presented as an A_i-module.

Lemma A.6. Let P be a module over a ring A. Then P is finitely generated and projective if and only if it is finitely presented and flat.

Proof. The direct implication was already proven in Theorem 3.1 and Observation 3.2. Let's prove the reverse implication. We begin proving that we can extend the result of Lemma 3.7 to the case that P is finitely presented (instead of finitely generated projective): Let P be a finitely presented A-module, and M a flat A-module. We claim that the map

$$\begin{aligned} \phi : P^* \otimes_A M &\longrightarrow \mathrm{Hom}_A(P, M) \\ f \otimes m &\longmapsto \phi(f \otimes m) : P \longrightarrow M \\ &\qquad\qquad\qquad\quad p \longmapsto f(p)m \end{aligned}$$

is an isomorphism. Note that we already know that the free case works (c.f. the proof of Lemma 3.7). In the general case, choose an exact sequence $A^m \to A^n \to P \to 0$. Then, we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & P^* \otimes_A M \arrow[r] \arrow[d] & (A^n)^* \otimes_A M \arrow[r] \arrow[d] & (A^m)^* \otimes_A M \arrow[d] \\
0 \arrow[r] & \mathrm{Hom}_A(P, M) \arrow[r] & \mathrm{Hom}_A(A^n, M) \arrow[r] & \mathrm{Hom}_A(A^m, M)
\end{tikzcd}$$

As the last two vertical arrows are isomorphisms, th first one must also be an isomorphism, and this proves the claim. Now given P finitely presented and flat, and applying the claim to $M = P$, we can find an element $\sum_{i=1}^t f_i \otimes p_i \in P^* \otimes_A P$ such that $\phi(\sum_{i=1}^t f_i \otimes p_i) = \mathrm{id}_P$, that is, $\sum_{i=1}^t f_i(x) \otimes p_i = x \ \forall x \in P$.

Therefore the A-linear maps $f : P \to A^t$, $f(x) = (f_i(x))_{i=1}^t$ and $g : A^t \to P$, $g((a_i)_{i=1}^t) = \sum_{i=1}^t a_i p_i$ satisfy $gf = \mathrm{id}$, and therefore g is surjective and the sequence

$$0 \to \ker g \to A^t \to P \to 0$$

splits, which implies that $P \oplus \ker g \cong A^t$, and so P is projective. □

Corollary A.2. A morphism of schemes is finite and locally free if and only if it is finitely presented and flat.

Definition A.3. A morphism of schemes $f : Y \to X$ is *étale* if and only if it is flat and unramified.

Theorem A.1. *i) A morphism of schemes is finite étale if and only if it is finitely presented and étale.*

ii) Let X be a locally noetherian scheme. Then a morphism of schemes $f : Y \to X$ is finite étale if and only if it is finite and étale.

Proof. i) By Corollary A.2, a morphism of schemes is finitely presented and étale if and only if it is finite and locally free and unramified. As finite étale morphisms are also finite and locally free, and all the definitions are local, it is enough to prove that an A-algebra B that is finitely generated and free is separable over A if and only if $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is unramified.

We will first reduce the problem to the case where A is a field. Using [1], Proposition 3.10, it can be seen that given M, N be finitely generated and free A-modules, and $f : M \to N$ an A-linear map, f is an isomophism if and only if for each $\mathfrak{p} \in \mathrm{Spec}(A)$ the induced map $A \otimes_A k(\mathfrak{p}) \to N \otimes_A k(\mathfrak{p})$ is an isomorphism. Therefore the morphism $\phi : B \to \mathrm{Hom}_A(B, A)$ of the definition of separability is an isomorphism if and only if $B \otimes_A k(\mathfrak{p}) \to \mathrm{Hom}_{k(\mathfrak{p})}(B \otimes_A k(\mathfrak{p}), k(\mathfrak{p}))$ is an isomorphism, that is, B is separable if and only if $B \otimes k(\mathfrak{p})$ is separable over $k(\mathfrak{p})$. It is also clear that $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is unramified if and only if $\mathrm{Spec}((B \otimes_A k(\mathfrak{p})) \to \mathrm{Spec}(k(\mathfrak{p}))$ is unramified for every prime $\mathfrak{p}$. This reduces the problem to the field case.

In that case, we can write $B = \prod_{i=1}^n B_i$, where each B_i is a local ring with nilpotent maximal ideals (c.f. [1], Theorem 8.7). Then B_i are the localizations of B in the primes $\mathfrak{q}$ of $\mathrm{Spec}(B)$. Therefore $\mathrm{Spec}(A) \to \mathrm{Spec}(B)$ is unramified if and only if B_i is a separable field extension of A for every i. Then Lemma 2.1 concludes the proof.

ii) It's enough to observe that if A is a noetherian ring, then A^n is a Noetherian module, and therefore, every submodule will be finitely generated. In particular, for every finitely generated module M over A, we can define the canonical surjective map $f : A^n \to M$, for a certain $n < \infty$. Then, the exact sequence

$$0 \to \ker f \to A^n \to M \to 0$$

implies that $\ker f$ is a submodule of A^n and, therefore, finitely generated. This implies that every finitely generated module is finitely presented, which concludes the proof.

□