Galois Theory for Schemes

Shan Gao

A Thesis

in the Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science (Mathematics) at
Concordia University
Montreal, Quebec, Canada
August 2012

CONCORDIA UNIVERSITY
SCHOOL OF GRADUATE STUDIES

This is to verify that the thesis prepared

By: **Shan Gao**

Entitled: **Galois Theory for Schemes**

and submitted in partial fulfilment of requirements for the degree of

Master of Science (Mathematics)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Dr. H. Kisilevsky ______________________ Examiner

Dr. C. David ______________________ Examiner

Dr. A. Iovita ______________________ Supervisor

Approved by Dr. J. Garrido ______________________
Chair of Department or Graduate Program Director

__________2012_____ Dr. B. Lewis ______________________
Dean of Faculty

ABSTRACT

Galois Theory for Schemes

Shan Gao

Given a connected scheme X, we consider the category of finite étale coverings of X. We will show that this category is equivalent to the category π-**Sets** of finite sets on which π acts continuously, where π is a profinite group, uniquely determined up to isomorphism. Our technique is to develop a basic theory for Galois category and show that category of finite étale coverings of X is a Galois category.

Keywords: Galois category; Fundamental group; Separable algebra; Finite Étale morphism

Contents

Introduction

In this thesis we study the basics of finite étale morphisms. It is the first step to study étale cohomology, which is a vast and extremely rich area of mathematics, with many applications. In this thesis we prove the main theorem of Galois theory for schemes, which classifies the finite étale coverings of a connected scheme X in terms of its fundamental group $\pi(X)$.

Our main aim in this thesis is to develop and study the theory of finite étale morphisms using a basic material in H. W. Lenstra's notes found at:

http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf.

There are no new results here. We have written the theory as we understood it and added most of the details which were left as exercises in Lenstra's notes.

The thesis is organized as follows. In Chapter 1, we give a brief review of the covering spaces and fundamental groups of topological spaces. The following chapter contains an axiomatic characterization of categories that are equivalent to π-**Sets** for some profinite group π. In Chapter 3, we treat the basic properties of finite étale morphisms, which generalize the properties of projective separable algebras. In the last chapter, we prove the main theorem of this thesis, by showing that the category of finite étale coverings of a connected scheme is a Galois category.

I would like to thank my supervisor, Professor Adrian Iovita, for numerous helpful discussions.

Chapter 1

The topological fundamental group

1.1 The fundamental group

In this section we will give a brief review of the construction of the fundamental group of a topological space. We shall assume that all spaces in this section are topological spaces and all maps are continuous. We set $I = [0, 1]$. For the details of this section we refer to Armstrong (1983) (Chapter 5), Massey (1991) (Chapter II).

Definition 1.1.1. Two maps $f_0, f_1 : X \to Y$ are said to be *homotopic* if there exists a map $F : X \times I \to Y$ such that $F(x, 0) = f_0(x)$ and $F(x, 1) = f_1(x)$ for all $x \in X$. The map F is called a *homotopy* from f_0 to f_1 and we shall write $f_0 \underset{F}{\simeq} f_1$.

Definition 1.1.2. A *path* in a space X is a map $f : I \to X$. A *loop* in X is a map $f : I \to X$ where $f(0) = f(1)$, and we shall say that the loop is *based* at the point $x_0 = f(0)$, which is referred to as the *basepoint*.

Definition 1.1.3. Two paths $f, g : I \to X$ are said to be *path homotopic*, denoted by $f \underset{(p)}{\simeq} g$, if

$f(0) = g(0)$, $f(1) = g(1)$ and there exists a map $F : I \times I \to X$ such that

$$\left.\begin{aligned} F(s,0) &= f(s) \\ F(s,1) &= g(s) \end{aligned}\right\} \text{ for all } s \in I,$$

$$\left.\begin{aligned} F(0,t) &= f(0) = g(0) \\ F(1,t) &= f(1) = g(1) \end{aligned}\right\} \text{ for all } t \in I.$$

Proposition 1.1.1. *Path homotopy is an equivalence relation.*

We denote $[f]$ to be the homotopy class of a path $f : I \to X$. If f and g are two paths in X where $f(1) = g(0)$ we define the *product* $f * g$ to be the path given by the formula

$$(f * g)(s) = \begin{cases} f(2s), & 0 \le s \le \frac{1}{2}, \\ g(2s-1), & \frac{1}{2} \le s \le 1. \end{cases}$$

We can see that this product operation respects homotopy classes, i.e. if $f_0 \underset{(p)}{\simeq} f_1$, $g_0 \underset{(p)}{\simeq} g_1$, and $f_0(1) = g_1(0)$ then $f_0 * g_0 \underset{(p)}{\simeq} f_1 * g_1$. Let X be a topological space, choose a base point $x_0 \in X$, and consider the set of all homotopy classes $[f]$ of loops $f : I \to X$ based at x_0. This set is denoted $\pi_1(X, x_0)$. We have the following theorem.

Theorem 1.1.1. $\pi_1(X, x_0)$ *is a group with respect to the product* $[f][g] = [f * g]$.

This group is called the *fundamental group* of X at the base point x_0.

1.2 Covering spaces

Definition 1.2.1. Let X be a topological space.

(1) A *space over* X is a topological space Y with a continuous map $p : Y \to X$.

(2) A morphism between two spaces $p_i : Y_i \to X$ $(i = 1, 2)$ over X is given by a continuous map

$f : Y_1 \to Y_2$ such that the following diagram

$$\begin{tikzcd} Y_1 \arrow[r, "f"] \arrow[dr, "p_1"'] & Y_2 \arrow[d, "p_2"] \\ & X \end{tikzcd}$$

commutes.

(3) A *covering space* of X is a space Y over X where the projection $p : Y \to X$ satisfies the following condition. For each point $x \in X$ there is an open neighborhood V, and a decomposition of $p^{-1}(V)$ as a family $(U_i)_{i \in D}$ of pairwise disjoint open subsets of Y, in such a way that the restriction of p to each U_i is a homeomorphism from U_i to V.

(4) A morphism between two covering spaces of X is a morphism of spaces over X.

Example 1.2.1. Take a nonempty discrete topological space D and form the topological product $X \times D$. The projection $X \times D \to X$ on the first coordiate turns $X \times D$ into a covering space over X. It is called a *trivial covering*.

Proposition 1.2.1. *A space Y over X is a covering if and only if each point of X has an open neighborhood V such that the restriction of the projection $p : Y \to X$ to $p^{-1}(V)$ is isomorphic (as a space over X) to a trivial cover.*

Proof. The "if" part is obvious by the previous example and the definition of covering. The "only if" part can be seen as follows: Given a cover $p : Y \to X$ and a decomposition $p^{-1}(V) \cong \coprod_{i \in D} (U_i)$ for some finite index set D, the map $f : \coprod_{i \in D} (U_i) \to V \times D$ defined by sending $u_i \in U_i$ to the pair $(p(u_i), i)$ is a homeomorphism, where D is endowed with the discrete topology. By construction this is an isomorphism of trivial covers of V. $\square$

Let X be a topological space and $\pi_1(X, x)$ be the fundamental group of X with base point x. Next we will show that given a cover $p : Y \to X$, there is a natural action by the group $\pi_1(X, x)$ on the fibre $p^{-1}(x)$. We need the following lemma.

Lemma 1.2.1. *Let $p : Y \to X$ be a cover, $y \in Y$ and $x = p(y)$.*

(1) Given a path $f : [0,1] \to X$ with $f(0) = x$, there is a unique path $\widetilde{f} : [0,1] \to Y$ with $\widetilde{f}(0) = y$ and $p \circ \widetilde{f} = f$.

(2) Assume moreover given a second path $g : [0,1] \to X$ homotopic to f. Then the unique $\widetilde{g} : [0,1] \to Y$ with $\widetilde{g}(0) = y$ and $p \circ \widetilde{g} = g$ has the same endpoint as $\widetilde{f}$, i.e. $\widetilde{f}(1) = \widetilde{g}(1)$.

Proof. For the proof of this lemma we refer to Massey (1991) (Chapter V, Section 3), Szamuely (2009) (Chapter 2, Section 2.3). ☐

We can now construct the left action of $\pi_1(X, x)$ on the fibre $p^{-1}(x)$.

Definition 1.2.2. Let $p : Y \to X$ be a covering space of X and $x \in X$. For any $y \in p^{-1}(x)$ and any $[f] \in \pi_1(X, x)$ represented by a loop f based at x, we define a left action of $\pi_1(X, x)$ on $p^{-1}(x)$ by $[f]y := \widetilde{f}(1)$, where $\widetilde{f}$ is the unique lifting given by the first part of the Lemma 1.2.1.

By the second part of the Lemma 1.2.1 we know that this definition does not depend on the choice of f. And $p\widetilde{f}(1) = f(1) = x$, i.e. $[f]y \in p^{-1}(x)$. So this action is well defined.

A space X is called *pathwise connected* if any two points of X can be joined by a path. A pathwise connected space is connected. A space is *locally pathwise connected* if each point has a basic family of pathwise connected neighborhoods. A space is *simply connected* if it has trivial fundamental group. A space is *semilocally simply connected* if every point $x \in X$ has a neighborhood U such that the natural homomorphism $\pi_1(U, x) \to \pi_1(X, x)$ is trivial.

If X is connected, locally pathwise connected, and semilocally simply connected, the group $\pi_1(X, x)$ is independent of the choice of x, up to isomorphism. Denoting it by $\pi_1(X)$ we have the following theorem.

Theorem 1.2.1. *Let X be a topological space satisfying the above conditions. Then the category of covers of X is equivalent to the category of $\pi_1(X)$-sets.*

All the details of the proof of the theorem above can be found in Massey (1991) (Ch V, Section 7), Szamuely (2009) (Ch2, Theorem 2.3.4).

In the Theorem 1.2.1, the fundamental group $\pi_1(X)$ has no topology and the $\pi_1(X)$-sets may not be finite. If X is connected the next theorem gives the relationship between the category of finite coverings of X and the category of $\widehat{\pi}(X)$**-Sets** for some profinite group $\widehat{\pi}(X)$.

Theorem 1.2.2. *Let X be a connected topological space. Then there exists a profinite group $\widehat{\pi}(X)$, uniquely determined up to isomorphism, such that the category of finite coverings of X is equivalent to the category $\widehat{\pi}(X)$**-sets** of finite sets on which $\widehat{\pi}(X)$ acts continuously.*

The proof of this theorem is given in Section 2.1.7. If X satisfies the conditions stated just before Theorem 1.2.1, then the group $\widehat{\pi}(X)$ that we get from Theorem 1.2.2 is the profinite completion of the fundamental group $\pi_1(X)$.

Chapter 2

Galois Categories

2.1 Galois Categories

2.1.1 Categories and Functors

A *category* $\mathcal{C}$ consists of a collection of objects $\mathrm{Ob}(\mathcal{C})$; and for two objects $A, B \in \mathrm{Ob}(\mathcal{C})$ a set $\mathrm{Mor}_{\mathcal{C}}(A, B)$ called the set of morphisms of A to B; and for three objects $A, B, C \in \mathrm{Ob}(\mathcal{C})$ a law of composition

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

satisfying the following axioms:

- Two sets $\mathrm{Mor}_{\mathcal{C}}(A, B)$ and $\mathrm{Mor}_{\mathcal{C}}(A', B')$ are disjoint unless $A = A'$ and $B = B'$, in which case they are equal.
- For each object A of $\mathcal{C}$ there is a morphism $\mathrm{id}_A \in \mathrm{Mor}_{\mathcal{C}}(A, A)$ which acts as left and right identity for the elements of $\mathrm{Mor}_{\mathcal{C}}(A, B)$ and $\mathrm{Mor}_{\mathcal{C}}(B, A)$ respectively, for all objects $B \in \mathrm{Ob}(\mathcal{C})$.
- The law of composition is associative (when defined), i.e. given $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$, $g \in$

$\mathrm{Mor}_{\mathcal{C}}(B, C)$ and $h \in \mathrm{Mor}_{\mathcal{C}}(C, D)$ then

$$(h \circ g) \circ f = h \circ (g \circ f),$$

for all objects A, B, C, D of $\mathcal{C}$.

Example 2.1.1. The following are some examples of categories:

(1) The category **Sets** of finite sets with maps of sets.

(2) Given a group G the category *G-Sets* of sets with a left G-action, with maps of sets that are compatible with G-action..

(3) Given a profinite group π the category of finite $\pi-$sets with a continuous left π-action together with maps between sets which are compatible with the π-action. We denote this category by **π-Sets**.

(4) The category of all finite coverings of a topological space X, denoted by $\mathbf{Cov}(X)$, with morphisms between coverings (see definition 1.2.1).

(5) The category of schemes with morphisms of schemes.

Definition 2.1.1. A morphism $u : X \to Y$ is an *isomorphism* of the category $\mathcal{C}$ if there exists a morphism $v : Y \to X$ such that $u \circ v = \mathrm{id}_Y$ and $v \circ u = \mathrm{id}_X$.

Let $\mathcal{C}, \mathcal{D}$ be categories. A *covariant (resp. contravariant) functor* F of $\mathcal{C}$ into $\mathcal{D}$ is a rule which to each object A in $\mathcal{C}$ associates an object $F(A)$ in $\mathcal{D}$, and to each morphism $f : A \to B$ associates a morphism $F(f) : F(A) \to F(B)$ (resp. $F(f) : F(B) \to F(A)$) such that:

- For all A in $\mathcal{C}$ we have $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$.
- If $f : A \to B$ and $g : B \to C$ are two morphisms of $\mathcal{C}$ then

$$F(g \circ f) = F(g) \circ F(f) \text{ (resp. } F(g \circ f) = F(f) \circ F(g)).$$

For categories $\mathcal{C}, \mathcal{D}$ and functors (say covariant) $F, G \colon \mathcal{C} \to \mathcal{D}$ a *natural transformation*, or a *morphism of functors* $\Phi : F \to G$ is a rule which to each object X of $\mathcal{C}$ associates a morphism $\Phi_X : F(X) \to G(X)$ such that for any morphism $f : X \to Y$ the following diagram is commutative:

$$\begin{tikzcd} F(X) \arrow[r, "\Phi_X"] \arrow[d, "F(f)"'] & G(X) \arrow[d, "G(f)"] \\ F(Y) \arrow[r, "\Phi_Y"] & G(Y) \end{tikzcd}$$

Definition 2.1.2. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor.

(1) We say F is *faithful* if for any objects X, Y of $\mathrm{Ob}(\mathcal{C})$ the map

$$F : \mathrm{Mor}_{\mathcal{C}}(X, Y) \to \mathrm{Mor}_{\mathcal{D}}(F(X), F(Y))$$

is injective.

(2) If these maps are all bijective then F is called *fully faithful.*

(3) The functor F is called *essentially surjective* if for any object $Y \in \mathrm{Ob}(\mathcal{D})$ there exists an object $X \in \mathrm{Ob}(\mathcal{C})$ such that $F(X)$ is isomorphic to Y in $\mathcal{D}$.

Definition 2.1.3. A functor $F : \mathcal{C} \to \mathcal{D}$ is called an *equivalence of categories* if there exists a functor $G : \mathcal{D} \to \mathcal{C}$ such that the compositions $F \circ G$ and $G \circ F$ are isomorphic to the identity functors $\mathrm{id}_{\mathcal{D}}$, respectively $\mathrm{id}_{\mathcal{C}}$. In this case we say that G is a *quasi-inverse* to F.

Lemma 2.1.1. *A functor is an equivalence of categories if and only if it is both fully faithful and essentially surjective.*

We refer Mac Lane (1998) (Ch IV, Section 4, Theorem 1) for the proof of this lemma.

2.1.2 Initial,Terminal object, Monomorphism and Epimorphism

Definition 2.1.4. Let $\mathcal{C}$ be a category.

(1) An object S of the category $\mathcal{C}$ is called an *initial* object if for every object X of $\mathcal{C}$ there is exactly one morphism $S \to X$.

(2) An object T of the category $\mathcal{C}$ is called a *terminal* object if for every object X of $\mathcal{C}$ there is exactly one morphism $X \to T$.

Note that, from the definition above, initial or terminal object is unique up to isomorphism if exists. We denote initial and terminal objects by $\mathbf{0}_{\mathcal{C}}$ and $\mathbf{1}_{\mathcal{C}}$ respectively. In **Sets** the empty set $\emptyset$ is an initial object, and any *singleton*, i.e., a set with one element, is a terminal object.

Definition 2.1.5. Let $\mathcal{C}$ be a category, and let $f : X \to Y$ be a morphism of $\mathcal{C}$.

(1) We say that f is a *monomorphism* if for every object Z and every pair of morphisms $u, v : Z \to X$ with $f \circ u = f \circ v$ we have $u = v$.

(2) We say that f is an *epimorphism* if for every object W and every pair of morphisms $u, v : Y \to W$ with $u \circ f = v \circ f$ we have $u = v$.

Example 2.1.2. In **Sets** the monomorphisms correspond to injective maps and the epimorphisms correspond to surjective maps.

We can see that the composition of monomorphisms (resp. epimorphisms) is still a monomorphism (resp. epimorphism).

Definition 2.1.6. Let $\mathcal{C}$ be a category. A *subobject* of an object X of $\mathcal{C}$ is a monomorphism $Y \to X$. A morphism of two subobjects $Y \to X$, $Y' \to X$ of X is a morphism $f : Y \to Y'$ in $\mathcal{C}$ making the diagram

$$\begin{tikzcd} Y \arrow[rr, "f"] \arrow[dr] & & Y' \arrow[dl] \\ & X & \end{tikzcd}$$

commute.

2.1.3 Products, Fibre products, Coproducts and Equalizers

Definition 2.1.7. Let $X, Y \in \mathrm{Ob}(\mathcal{C})$, A *product* of X and Y is an object $X \times Y \in \mathrm{Ob}(\mathcal{C})$ together with morphisms $p \in \mathrm{Mor}_{\mathcal{C}}(X \times Y, X)$ and $q \in \mathrm{Mor}_{\mathcal{C}}(X \times Y, Y)$ such that the following universal property holds: For any $Z \in \mathrm{Ob}(\mathcal{C})$ and morphisms $\alpha \in \mathrm{Mor}_{\mathcal{C}}(Z, X)$ and $\beta \in \mathrm{Mor}_{\mathcal{C}}(Z, Y)$ there is a unique $\gamma \in \mathrm{Mor}_{\mathcal{C}}(Z, X \times Y)$ making the diagram

$$\begin{tikzcd} & Z \arrow[dl, "\alpha"'] \arrow[d, dashed, "\gamma"] \arrow[dr, "\beta"] & \\ X & X \times Y \arrow[l, "p"] \arrow[r, "q"'] & Y \end{tikzcd}$$

commute.

We can similarly define a product of an arbitrary family of objects.

Definition 2.1.8. Let $(A_i)_{i \in I}$ be a collection of objects of a category $\mathrm{Ob}(\mathcal{C})$. The *product* of the A_i is a pair $(A, (p_i)_{i \in I})$ consisting of an object A and a family of morphisms $\{p_i : A \to A_i\}$ satisfying the following property: Given a family of morphisms $\{g_i : B \to A_i\}$, there exists a unique morphism $\gamma : B \to A$ such that $p_i \circ \gamma = g_i$ for all i. The product of (A_i) will be denoted by $\prod_{i \in I} A_i$.

The empty collection of objects has a product if and only if $\mathcal{C}$ has an terminal object. If I is finite, $I = \{i_1, i_2, \ldots, i_n\}$, we may write $A_{i_1} \times A_{i_2} \times \cdots \times A_{i_n}$ instead of $\prod_{i \in I} A_i$.

Definition 2.1.9. Let $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$, $f \in \mathrm{Mor}_{\mathcal{C}}(X, Z)$ and $g \in \mathrm{Mor}_{\mathcal{C}}(Y, Z)$. A *fibre product* of f and g is an object $X \times_Z Y \in \mathrm{Ob}(\mathcal{C})$ together with morphisms $p_1 \in \mathrm{Mor}_{\mathcal{C}}(X \times_Z Y, X)$ and $p_2 \in \mathrm{Mor}_{\mathcal{C}}(X \times_Z Y, Y)$ making the diagram

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

commute, and such that the following universal property holds: For any $T \in \mathrm{Ob}(\mathcal{C})$ and morphisms $\alpha \in \mathrm{Mor}_{\mathcal{C}}(T, X)$ and $\beta \in \mathrm{Mor}_{\mathcal{C}}(T, Y)$ with $f \circ \alpha = g \circ \beta$ there is a unique $\phi \in \mathrm{Mor}_{\mathcal{C}}(T, X \times_Z Y)$

making the following diagram

$$\begin{tikzcd} T \arrow[dr, dashed, "\phi"] \arrow[drr, bend left, "\beta"] \arrow[ddr, bend right, "\alpha"'] & & \\ & X \times_Z Y \arrow[r, "p_2"'] \arrow[d, "p_1"] & Y \arrow[d, "g"] \\ & X \arrow[r, "f"] & Z \end{tikzcd}$$

commute.

Definition 2.1.10. We say the category $\mathcal{C}$ *has fibre products* if the fibre product exists for any $f \in \mathrm{Mor}_{\mathcal{C}}(X, Z)$ and $g \in \mathrm{Mor}_{\mathcal{C}}(Y, Z)$.

The fibre product is uniquely determined up to isomorphism, if it exists. If a category $\mathcal{C}$ has fibre products and terminal objects, then $X \times Y$ is just $X \times_{1_{\mathcal{C}}} Y$. In **Sets** the fibre product $X \times_Z Y$ is the set of all pairs (x, y) in the Cartesian product of X and Y for which x and y have the same image in Z. If the maps $X \to Z$, $Y \to Z$ are inclusions this may be identified with the intersection of X and Y.

Definition 2.1.11. Let $(A_i)_{i \in I}$ be a collection of objects of a category $\mathrm{Ob}(\mathcal{C})$. The *coproduct*, or *amalgamated sum* of the A_i is a pair $(S, (f_i)_{i \in I})$ consisting of an object S and a family of morphisms $\{f_i : A_i \to S\}$ satisfying the following property: Given a family of morphisms $\{g_i : A_i \to C\}$, there exists a unique morphism $\gamma : S \to C$ such that $\gamma \circ f_i = g_i$ for all i. The coproduct of (A_i) will be denoted by $\coprod_{i \in I} A_i$.

The sum is unique up to isomorphism if it exists. In the category of sets the sum of the A_i is their disjoint union.

Definition 2.1.12. We say that *finite sum exists* in $\mathcal{C}$ if any finite collection of objects has a sum in $\mathcal{C}$.

The empty collection of objects has a sum if and only if $\mathcal{C}$ has an initial object. If I is finite, $I = \{i_1, i_2, \ldots, i_n\}$, we may write $A_{i_1} \amalg A_{i_2} \amalg \cdots \amalg A_{i_n}$ instead of $\coprod_{i \in I} A_i$.

Definition 2.1.13. A morphism $u : X \to Y$ in a category $\mathcal{C}$ is called an isomorphism of X with a direct summand of Y if there exists a morphism $q_2 : Z \to Y$ such that Y, together with $q_1 = u$ and q_2, is the sum (or coproduct) of X and Z.

In **Sets**, we can simply get this by letting $Z = Y - u(X)$.

Definition 2.1.14. Suppose that X, Y are objects of a category $\mathcal{C}$ and $u, v : X \to Y$ are morphisms. We say a pair (E, e) is an *equalizer* for the pair (u, v) if $e : E \to X$ is a $\mathcal{C}$-morphism, $u \circ e = v \circ e$ and if (E, e) satisfies the following universal property: For every morphism $f : W \to X$ in $\mathcal{C}$ such that $u \circ f = v \circ f$ there exists a unique morphism $\phi : W \to E$ such that $f = e \circ \phi$.

As in the case of the fibre product above, equalizers when they exist are unique up to unique isomorphism. In **Sets** the equalizer of $A \underset{g}{\overset{f}{\rightrightarrows}} B$ is the subset $\{a \in A \mid f(a) = g(a)\}$ of A with the inclusion. We have the following properties of equalizers.

Proposition 2.1.1. *If (E, e) is an equalizer of $X \underset{g}{\overset{f}{\rightrightarrows}} Y$, then (E, e) is a subobject of X. Any two equalizers of $X \underset{g}{\overset{f}{\rightrightarrows}} Y$ are isomorphic subobjects of X.*

Proposition 2.1.2. *If (E, e) is an equalizer of $X \underset{g}{\overset{f}{\rightrightarrows}} Y$, then the following are equivalent:*

(1) $f = g$.

(2) e is an isomorphism.

(3) e is an epimorphism.

For the proof of these two propositions, we refer to Herrlich and Strecker (1973) (Ch VI, 16.7 Proposition)

2.1.4 Quotient under group actions

Definition 2.1.15. Let Y be an object of a category $\mathcal{C}$ and $G \subset \mathrm{Aut}_{\mathcal{C}}(Y)$ a finite subgroup of the group of automorphisms of Y in $\mathcal{C}$. The *quotient of Y by G* is an object in $\mathcal{C}$, denoted by Y/G, along with a morphism $\rho : Y \to Y/G$ satisfying $\rho \circ \sigma = \rho$ for all $\sigma \in G$ and the universal property: If Z is an object of $\mathcal{C}$ and $f : Y \to Z$ satisfies $f \circ \sigma = f$ for all $\sigma \in G$, then there is a unique morphism $g : Y/G \to Z$ such that $f = g \circ \rho$.

Example 2.1.3. For any object Y of the category **Sets** of finite sets, the finite subgroup $G \subset \mathrm{Aut}_{\mathbf{Sets}}(Y)$ acts on Y and Y/G is the set of G-orbits of Y.

2.1.5 Galois categories

Definition 2.1.16. Let $\mathcal{C}$ be a category and F a covariant functor from $\mathcal{C}$ to the category **Sets** of finite sets. We say that $\mathcal{C}$ is a *Galois category* with *fundamental functor* F if the following six axioms are satisfied.

(G1) There is a terminal object in $\mathcal{C}$, and the fibre product of any two objects over a third one exists in $\mathcal{C}$.

(G2) Finite sums exist in $\mathcal{C}$, in particular an initial object, and for any object in $\mathcal{C}$ the quotient by a finite group of automorphisms exists.

(G3) Any morphism $X \xrightarrow{u} Y$ in $\mathcal{C}$ can be factored as

$$\begin{tikzcd} X \arrow[rr, "u"] \arrow[dr, "u_1"'] & & Y \\ & Y_1 \arrow[ur, hook, "u_2"'] & \end{tikzcd}$$

where u_1 is an epimorphism, u_2 is a monomorphism and $Y = Y_1 \amalg Y_2$, $Y_2 \in \mathcal{C}$.

(G4) The functor F maps terminal objects to terminal objects and commutes with fibre products.

(G5) The functor F commutes with finite sums and quotients (see Definition 2.1.15), maps epimorphisms to epimorphisms.

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

It is easy to see that the category **Sets** with the identity functor is a Galois category.

2.1.6 The automorphism group of a fundamental functor

Let $\mathcal{C}$ be a Galois category with fundamental functor F. An automorphism of F is an invertible natural transformation of functors $F \to F$. Equivalently, an automorphism σ of F is a collection of bijections $\sigma_X : F(X) \to F(X)$, one for each $X \in \mathrm{Ob}(\mathcal{C})$, such that for each $\mathcal{C}$-morphism $Y \xrightarrow{f} Z$ the diagram

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

is commutative. Let $S_{F(X)}$ denote the permutation group of $F(X)$. It is finite since $F(X)$ is. Then there is a natural injection:

$$\mathrm{Aut}(F) \hookrightarrow \textstyle\prod_{X \in \mathcal{C}} S_{F(X)}$$

given by $\sigma \mapsto (\sigma_X)_X$, where $\mathrm{Aut}(F)$ is the group of all automorphisms of F. It is supposed here that $\mathcal{C}$ is a small category, i.e. its objects form a set. Given each $S_{F(X)}$ the discrete topology and endow $\prod\limits_{X \in \mathcal{C}} S_{F(X)}$ with the product topology, the product above will be a profinite group.

For each $\mathcal{C}-$morphism $g : Y \to Z$, we define a subset as:

$$\Gamma_g = \left\{ (\sigma_X) \in \prod_{X \in \mathcal{C}} S_{F(X)} \;\middle|\; \sigma_Z F(g) = F(g) \sigma_Y \right\}.$$

Γ_g is closed in the product since only two coordinates have been restricted. Then

$$\mathrm{Aut}(F) = \bigcap_{g : Y \to Z} \Gamma_g$$

is a closed subproup of profinite group $\prod_{X \in \mathcal{C}} S_{F(X)}$ hence is profinite. Since we may replace $\mathcal{C}$ by an equivalent category, the foregoing is also valid if $\mathcal{C}$ is essentially small instead of small.

Let $\pi = \mathrm{Aut}(F)$. There is a natural action of π on $F(X)$ given by: $\sigma \cdot t = \sigma_X(t)$ for each $X \in \mathrm{Ob}(\mathcal{C})$, $\sigma \in \mathrm{Aut}(F)$ and $t \in F(X)$. Then the kernel of this action

$$\mathrm{Ker}(\pi) \;=\; \left\{ \sigma \in \pi \;\middle|\; \sigma t = t \text{ for all } t \in F(X) \right\}$$

$$
\begin{aligned}
&= \pi \cap \left\{ (\sigma_Y) \in \prod_{Y \in \mathcal{C}} S_{F(Y)} \;\middle|\; \sigma_X(t) = t \text{ for all } t \in F(X) \right\} \\
&= \pi \cap \prod_{Y \in \mathcal{C}} U_Y,
\end{aligned}
$$

where $U_Y = S_{F(Y)}$ for $Y \neq X$ and $U_X = \{\sigma_X \in S_{F(X)} \mid \sigma_X(t) = t, \ \forall\, t \in F(X)\}$. This means that $\mathrm{Ker}(\pi)$ is open in $\prod_{Y\in\mathcal{C}} S_{F(Y)}$ under the product topology hence π acts continuously on $F(X)$ and gives $F(X)$ a π-set structure for $\forall X \in \mathrm{Ob}(\mathcal{C})$.

Given a $\mathcal{C}$-morphism $f : Y \to Z$, for any $\sigma \in \pi$, $t \in F(Y)$, we have

$$F(f)(\sigma t) = F(f)(\sigma_Y(t)) = (F(f)\sigma_Y)(t) = (\sigma_Z F(f))(t) = \sigma_Z(F(f)(t)).$$

This shows that $F(f)$ is compatible with the π-action defined above. Now we may regard F as a functor $H : \mathcal{C} \to \pi$-**Sets** by $H(X) = F(X)$ and $H(f : X \to Y) = (F(f) : F(X) \to F(Y))$, and that F is the composite of H and the forgetful functor π-**Sets** $\to$ **Sets**. We have the following theorem.

Theorem 2.1.1. *Let $\mathcal{C}$ be an essentially small Galois category with fundamental functor F. Then we have:*

*(a) The functor $H : \mathcal{C} \to \pi$-**Sets** defined above is an equivalence of categories;*

*(b) If π' is a profinite group such that the categories $\mathcal{C}$ 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 $\pi = \mathrm{Aut}(F)$;*

(c) If F' is a second fundamental functor on $\mathcal{C}$, then F and F' are isomorphic;

*(d) If π' is a profinite group such that the categories $\mathcal{C}$ and π'-**Sets** are equivalent, then there is an isomorphism of profinite groups $\pi' \cong \pi$ which is canonically determined up to an inner automorphism of π.*

For the proof of this theorem, see Section 2.2. Next, we will show that the category $\mathbf{Cov}(X)$ (see example 2.1.1) with X connected, is a Galois category and we will give the proof of Theorem 1.2.2.

2.1.7 Finite coverings

Let X be a topological space, $x \in X$, and $\mathbf{Cov}(X)$ the category of finite coverings of X. Let $F_x : \mathbf{Cov}(X) \to \mathbf{Sets}$ be the functor sending a cover $f : X \to Y$ to the fibre $f^{-1}(x)$. We shall prove that, given X connected, $\mathbf{Cov}(X)$ is a Galois category with fundamental functor F_x. Then we can deduce Theorem 1.2.2 from Theorem 2.2.1. We need to check the axioms $(G1)-(G6)$ in Definition 2.1.16. First, we present several lemmas.

Lemma 2.1.2. *Let X, Y, Z be topological spaces, $f : Y \to X$, $g : Z \to X$ be finite coverings, and $h : Y \to Z$ a continuous map with $f = gh$. Then for any $x \in X$, there exists an open neighborhood U of x in X such that f, g and h are trivial above U, i.e., there exist finite discrete sets D and E, homeomorphisms $\alpha : f^{-1}(U) \to U \times D$ and $\beta : g^{-1}(U) \to U \times E$ and a map $\phi : D \to E$ such that the diagram*

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

is commutative where the maps $U \times D \to U$ and $U \times E \to U$ are the projections on the first coordinate.

Proof. By Proposition 1.2.1, we can find neighborhoods V' and V'' of x in X, finite discrete sets D, E and homeomorphisms $\alpha : f^{-1}(V') \to V' \times D$, $\beta : g^{-1}(V'') \to V'' \times E$, such that the diagrams

$$\begin{tikzcd}
f^{-1}(V') \arrow[rr, "\sim", "\alpha"'] \arrow[dr, "f"'] & & V' \times D \arrow[dl] \\
& V' &
\end{tikzcd}
\qquad
\begin{tikzcd}
g^{-1}(V'') \arrow[rr, "\sim", "\beta"'] \arrow[dr, "g"'] & & V'' \times E \arrow[dl] \\
& V'' &
\end{tikzcd}$$

commute. First we let $V = V' \cap V''$. Then we have the following commutative diagram

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

We can get a continuous map $\beta h \alpha^{-1} : V \times D \to V \times E$. It respects the projections to V so the pair $(v, d) \in V \times D$ will be sent to $(v, \phi_v(d)) \in V \times E$ for some $\phi_v(d) \in E$. For any fixed v this will define a map $\phi_v : D \to E$ by sending d to $\phi_v(d)$. Let $\phi = \phi_x$. The two maps $V \times D \longrightarrow D \xrightarrow{\phi} E$ and $V \times D \xrightarrow{\beta h \alpha^{-1}} V \times E \longrightarrow E$ combine into a continuous map $V \times D \to E \times E$: $(v, d) \mapsto (\phi(d), \phi_u(d))$. The image of $\{x\} \times D$ under this map will be contained in the diagonal of $E \times E$, which is open. Then there exists an neighborhood of $\{x\} \times D$ in $V \times D$ whose image is also in the diagonal. Since D is finite, we can take this neighborhood to be the form $U \times D$, with U a neighborhood of x in X. Replacing V by U we can prove Lemma 2.1.2. $\square$

Remark 2.1.1. From this lemma, we can get that under the assumptions of Lemma 2.1.2, $h : Y \to Z$ is also a finite covering since $U \times D \xrightarrow{\mathrm{id}_U \times \phi} U \times E$ is a trivial cover.

The following lemma is called *the gluing lemma*. The proof can be found in Armstrong (1983), Chapter 4, Section 4.2.

Lemma 2.1.3. *Suppose $X = A \cup B$ where $A,\ B \subseteq X$ are closed. If $f : X \to Y$ is continuous when restricted to A and to B, then f is continuous on X.*

Lemma 2.1.4. *Let X be a topological space and $f : Y \to X$ a finite covering. Then f is both open and closed.*

Proof. This property can be checked locally on X so we can assume that $f : Y \to X$ is a finite trivial cover, i.e., $Y \cong X \times D$ for some finite discrete set D. For any open $U \subseteq Y$ and $\forall x \in f(U)$, we can write $U = U_1 \amalg U_2 \amalg \cdots \amalg U_n$ where $n = |D|$, the cardinality of the set D and U_i is open in X for $i = 1, 2, \ldots, n$. Then $V = \bigcap_{i=1}^{n} U_i$ is a neighborhood of x in X and $V \subseteq f(U)$. This implies that f is open. Similarly we can show that f is closed. $\square$

Lemma 2.1.5. *Let X be a topological space. If $g : Y \to Z$, $h : W \to Z$ are morphisms in $\mathcal{C}$, then the fibre product $Y \times_Z W$, which is defined by*

$$Y \times_Z W = \Big\{(y, w) \in Y \times W \;\Big|\; g(y) = h(w) \text{ in } Z\Big\},$$

is a finite covering of X with the obvious map.

Proof. Let $x \in X$. We can find a neighborhood U of x in X such that the covering $Y \to X$, $Z \to X$ and the map $g : Y \to Z$ are trivial in the sense of Lemma 2.1.2. By shrinking U to a neighborhood small enough, we can assume the cover $W \to X$ and the map $h : W \to Z$ are trivial on U, too. We have the following commutative diagram:

$$\begin{tikzcd}
& U \times D' \arrow[d, "\mathrm{id}_U \times \phi'"'] \arrow[ddr] & \\
U \times D \arrow[r, "\mathrm{id}_U \times \phi"] \arrow[drr] & U \times E \arrow[dr] & \\
& & U
\end{tikzcd}$$

Then the fibre product $Y \times_Z W$ is just $U \times (D \times_E D')$ locally, where $D \times_E D'$ is the fibre product of $\phi : D \to E$ and $\phi' : D' \to E$ in the category **Sets**. It is obvious that $U \times (D \times_E D') \to U$ is a trivial cover. Then by Proposition 1.2.1 $Y \times_Z W$ is an object in $\mathbf{Cov}(X)$. $\square$

Lemma 2.1.6. *Let X be a topological space and $h : Y \to Z$ is a morphism in $\boldsymbol{Cov}(X)$. Then h is injective if and only if it is a monomorphism and that h is surjective if and only if it is an epimorphism.*

Proof. From Lemma 2.1.4 we can see that $h(Y)$ is open and closed in Z.

- (injection $\Longleftrightarrow$ monomorphism)

  "$\Rightarrow$" Suppose h is injective. If for any W in $\mathbf{Cov}(X)$ and morphisms $\varphi_1,\ \ \varphi_2 : W \to Y$, such that $h\varphi_1 = h\varphi_2$, then for each $w \in W$, we have $h\varphi_1(w) = h\varphi_2(w)$. Since h is injective, we have $\varphi_1(w) = \varphi_2(w)$ hence $\varphi_1 = \varphi_2$ and h is a monomorphism.

"$\Leftarrow$" Suppose h is a monomorphism in $\mathbf{Cov}(X)$. Consider the following commutative diagram:

$$\begin{tikzcd} Y \times_Z Y \arrow[r, "p_2"] \arrow[d, "p_1"'] & Y \arrow[d, "h"] \\ Y \arrow[r, "h"] & Z \end{tikzcd}$$

Then $p_1 = p_2$ since h is a monomorphism. If $h(y_1) = h(y_2)$ for some y_1, y_2 in Y, then $(y_1, y_2) \in Y \times_Z Y$. So we have $y_1 = p_1(y_1, y_2) = p_2(y_1, y_2) = y_2$ which implies that h is injective.

- (surjection $\Longleftrightarrow$ epimorphism)

"$\Rightarrow$" First, we assume h is surjective. Suppose now we have two compositions

$$\begin{tikzcd} Y \arrow[r, "h"] & Z \arrow[r, shift left, "\alpha"] \arrow[r, shift right, "\beta"'] & W \end{tikzcd}$$

with $\alpha \circ h = \beta \circ h$. For any $z \in Z$, there exists a $y \in Y$, such that $h(y) = z$. Then $\alpha(z) = \alpha h(y) = \beta h(y) = \beta(z)$, i.e., $\alpha = \beta$ which implies that h is an epimorphism.

"$\Leftarrow$" Suppose h is an epimorphism now. Let $Z_0 = \{z \in Z \ : \ |h^{-1}(z)| = 0\}$ and $Z_1 = Z - Z_0$ be subsets of Z, where $|h^{-1}(z)|$ denotes the cardinality of the set $h^{-1}(z)$. Then $Z_1 = h(Y)$ is an open and closed subspace in Z. We have two compositions:

$$\begin{tikzcd} Y \arrow[r, "h"] & Z = Z_0 \amalg Z_1 \arrow[r, shift left] \arrow[r, shift right] & Z_0 \amalg Z_0 \amalg Z_1 . \end{tikzcd}$$

Since h is an epimorphism, the two natural maps $Z = Z_0 \amalg Z_1 \rightrightarrows Z_0 \amalg Z_0 \amalg Z_1$ must be equal. This implies $Z_0 = \emptyset$ hence h is a surjection.

□

Next we will check the axioms $(G1) - (G6)$ (see Definition 2.1.16) to show that $\mathbf{Cov}(X)$ with functor F_x defined in the beginning of this section is a Galois category if X is connected.

(G1) • The trivial cover $\mathrm{id}_X : X \to X$ is clearly a terminal object of $\mathbf{Cov}(X)$.

• By lemma 2.1.5 the fibre product of any two objects over a third one exists in $\mathbf{Cov}(X)$.

(G2) • The finite sum of $f_i : X_i \to X$, $i \in I$, is $f : \coprod_{i\in I} X_i \to X$, the disjoint union with the usual topology and $f\big|_{X_i} = f_i$. By the gluing lemma (see Lemma 2.1.3), $\coprod_{i\in I} X_i$ is a finite cover of X.

• The initial object is the empty cover $f : \emptyset \to X$.

• The quotient of $p : Y \to X$ by a finite subgroup G of the automorphisms of this covering is the set of orbits of Y under G, given the quotient topology. The quotient space is a finite cover of X in an obvious way.

(G3) Let $h : Y \to Z$ be a morphism in $\mathbf{Cov}(X)$. We can get a factorization of h as:

$$\begin{tikzcd} Y \arrow[rr, "h"] \arrow[dr, "h_1"'] & & Z = Z_1 \amalg Z_0 \\ & Z_1 \arrow[ur, hook, "h_2"'] & \end{tikzcd}$$

where Z_1, Z_0 as in Lemma 2.1.6 with h_1 epimorphism and h_2 monomorphism.

(G4) • $F_x(\mathbf{1}_{\mathbf{Cov}(X)}) = F_x(\mathrm{id}_X : X \to X) = \mathrm{id}_X^{-1}(x) = \{x\} = \mathbf{1}_{\mathbf{Sets}}$.

• Suppose we have the following commutative diagram:

$$\begin{tikzcd} Y \times_Z W \arrow[r, "p_1"] \arrow[d, "p_2"'] & Y \arrow[d, "g"] \arrow[dr, bend left, "f_1"] & \\ W \arrow[r, "h"] \arrow[drr, bend right, "f_2"'] & Z \arrow[dr, "f"] & \\ & & X \end{tikzcd}$$

Then

$$\begin{aligned} F_x(Y \times_Z W) &= (fgp_1)^{-1}(x) = (f_1p_1)^{-1}(x) \\ &= \{(y, w) \mid h(w) = g(y), f_1p_1(y, w) = f_2p_2(y, w) = x\} \\ &= \{(y, w) \mid h(w) = g(y), f_1(y) = f_2(w) = x\} \end{aligned}$$

$$
\begin{aligned}
&= \{f_1^{-1}(x)\} \times_{\{f^{-1}(x)\}} \{f_2^{-1}(x)\} \\
&= F_x(Y) \times_{F_x(Z)} F_x(W).
\end{aligned}
$$

(G5) • First we show F_x commutes with finite sums:

$$
\begin{aligned}
& F_x(f : X_1 \amalg X_2 \amalg \cdots \amalg X_n \to X) = f^{-1}(x) \\
&= \{x_1 \in X_1 \mid f(x_1) = x\} \amalg \cdots \amalg \{x_n \in X_n \mid f(x_n) = x\} \\
&= \{x_1 \in X_1 \mid f_1(x_1) = x\} \amalg \cdots \amalg \{x_n \in X_n \mid f_n(x_n) = x\} \\
&= \{f_1^{-1}(x)\} \amalg \cdots \amalg \{f_n^{-1}(x)\} \\
&= F_x(X_1) \amalg \cdots \amalg F_x(X_n).
\end{aligned}
$$

• Since epimorphisms in both **Cov**(X) and **Sets** are surjections, it is obvious that F_x sends epimorphisms to epimorphisms.

• We now show that F_x commutes with quotients.

$$
\begin{aligned}
F_x(p_G : Y/G \to X) &= p_G^{-1}(x) = \{Gy \mid p_G(Gy) = x\} \\
&= \{Gy \mid p(y) = x\} \\
&= \{y \in Y \mid p(y) = x\}/G \\
&= F_x(Y)/G.
\end{aligned}
$$

(G6) Finally, assume X is connected. Let $Y \xrightarrow{h} Z$ is a morphism in **Cov**(X). Then $F_x(h)$ is just the restriction of h to the fibre of x in Y. This map is bijective if and only if the map ϕ from Lemma 2.1.2 is bijective. Let $X_1 = \{x \in X \mid F_x(h)$ is bijective $\}$ and $X_2 = \{x \in X \mid F_x(h)$ is not bijective $\}$. From Lemma 2.1.2 both X_1 and X_2 are open in X. Since X is connected and $F_x(h)$ is an isomorphism, $X_1 \neq \emptyset$. Hence $X_1 = X$ and h is a bijective. By Lemma 2.1.4 h is open, thus is an isomorphism in **Cov**(X).

Now, we have proved that **Cov**(X) is a Galois category if X is connected. Since every finite covering $Y \to X$ is equivalent to one in which the underlying set is a subset of $X \times \mathbb{Z}$, $\mathbf{Cov}(X)$ is essentially small. Then we can deduce Theorem 1.2.2 from Theorem 2.2.1.

2.2 Proof of Theorem2.2.1

The goal of this section is to prove the following theorem in details:

Theorem 2.2.1. *Let $\mathcal{C}$ be an essentially small Galois category with fundamental functor F. Then we have:*

*(a) The functor $H : \mathcal{C} \to \pi$-**Sets** defined above is an equivalence of categories;*

*(b) If π' is a profinite group such that the categories $\mathcal{C}$ 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 $\pi = \mathrm{Aut}(F)$;*

(c) If F' is a second fundamental functor on $\mathcal{C}$, then F and F' are isomorphic;

*(d) If π' is a profinite group such that the categories $\mathcal{C}$ and π'-**Sets** are equivalent, then there is an isomorphism of profinite groups $\pi' \cong \pi$ which is canonically determined up to an inner automorphism of π.*

We will see that each axiom of $(G1)-(G6)$ plays an important role in the proof. First we see some equivalent descriptions of some axioms and some properties of Galois category and fundamental functor. We will give the proof of the theorem as follows:

1. First we show that a Galois category is artinian (Def.2.2.1, Lemma 2.2.4).

2. We claim that the fundamental functor of a Galois category is strictly pro-representable (Def.2.2.2, Lemma 2.2.9).

3. We introduce the definition and some properties of connected objects (Def.2.2.3, Lemma 2.2.10).

4. We discuss Galois objects and their properties (Def.2.2.4, Lemma 2.2.11).

5. Finally we construct a profinite group π as required.

2.2.1 Properties of Galois category and Fundamental functor

Lemma 2.2.1. *Let $\mathcal{C}$ be a category. Then $\mathcal{C}$ satisfies $(G1)$ if and only if it has equalizers and finite products.*

Proof. "$\Rightarrow$" Suppose that $\mathcal{C}$ satisfies $(G1)$. It is easy to see that finite product exist since fibre product and terminal object exist. Now let $Y \overset{u}{\underset{v}{\rightrightarrows}} Z$ be morphisms in $\mathcal{C}$, we have the following commutative diagram:

$$\begin{tikzcd}
 & (Y \times_Z Y) \times_{Y\times Y} Y \arrow[rr, "p_2'"] \arrow[d, "p_1'"'] & & Y \arrow[d, "(\mathrm{id}_Y,\ \mathrm{id}_Y)"] \\
 & Y \times_Z Y \arrow[rr, "(p_1,\ p_2)"] \arrow[dl, "p_1"'] \arrow[dr, "p_2"] & & Y \times Y \\
Y \arrow[dr, "u"'] & & Y \arrow[dl, "v"] & \\
 & Z & &
\end{tikzcd}$$

For any $W \in \mathrm{Ob}(\mathcal{C})$ and any morphism $W \xrightarrow{f} Y$ with $uf = vf$, there exists a unique $\alpha : W \to Y \times_Z Y$ such that $p_1\alpha = p_2\alpha = f$. This implies that $(p_1,\ p_2)\alpha = (f, f) = (\mathrm{id}_Y,\ \mathrm{id}_Y)f$. So there exists a unique morphism $\phi : W \to (Y \times_Z Y) \times_{Y\times Y} Y$ such that the diagram

$$\begin{tikzcd}
(Y \times_Z Y) \times_{Y\times Y} Y \arrow[r, "p_2'"] & Y \arrow[r, shift left, "u"] \arrow[r, shift right, "v"'] & Z \\
W \arrow[u, dashed, "\exists\,!\ \phi"] \arrow[ur, "f"'] & &
\end{tikzcd}$$

commutes. This shows that $(Y \times_Z Y) \times_{Y\times Y} Y$ is an equalizer for $Y \overset{u}{\underset{v}{\rightrightarrows}} Z$.

"$\Leftarrow$" Now assume that $\mathcal{C}$ has equalizers and finite products. Taking the finite product over an empty set gives the terminal object. Next we suppose $X \xrightarrow{f} Z$ and $Y \xrightarrow{g} Z$ are morphisms in $\mathcal{C}$. Let p, q be the canonical projections $X \times Y \xrightarrow{p} X$, $X \times Y \xrightarrow{q} Y$. Let (E, e) be the equalizer of $X \times Y \underset{gq}{\overset{fp}{\rightrightarrows}} Z$. For any object W and morphism $\alpha : W \to X \times Y$ with $fp\alpha = gq\alpha$, there exists a unique morphism $\phi : W \to E$ such that $\alpha = e\phi$.

$$\begin{tikzcd}
W \arrow[dr, dashed, "\phi"] \arrow[drr, bend left, "q\alpha"] \arrow[ddr, bend right, "p\alpha"'] & & \\
& E \arrow[r, "qe"] \arrow[d, "pe"] & Y \arrow[d, "g"] \\
& X \arrow[r, "f"'] & Z
\end{tikzcd}$$

Hence E is the fibre product $X \times_Z Y$. $\square$

Remark 2.2.1. Let $\mathcal{C}$ be a category satisfying $(G1)$ and F a covariant functor from $\mathcal{C}$ to **Sets**. From this lemma we can conclude that $\mathcal{C}$ satisfies $(G4)$ if and only if F commutes with equalizers and with finite products.

Corollary 2.2.1. *Let $\mathcal{C}$ be a Galois category with fundamental functor F, then finite products and equalizers exist in $\mathcal{C}$ and F commutes with finite products and equalizers.*

Lemma 2.2.2. *Let $\mathcal{C}$ be a category and $F : \mathcal{C} \to$ **Sets** be a functor satisfying* $(G1)$, $(G4)$ *and* $(G6)$. *Let further $f : Y \to X$ be a morphism in $\mathcal{C}$. Then*

(a) f is a monomorphism if and only if the first projection $p_1 : Y \times_X Y \to Y$ is an isomorphism.

(b) f is a monomorphism if and only if F(f) is injective.

Proof. (a) "⇒" Suppose f is a monomorphism first. We have the following two commutative diagrams:

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

Since f is a monomorphism we have $p_1 = p_2$, hence $F(p_1) = F(p_2)$. By $(G4)$,

$$\begin{aligned} F(Y \times_X Y) &= F(Y) \times_{F(X)} F(Y) \\ &= \{(x, y) \mid F(f)(x) = F(f)(y)\}. \end{aligned}$$

For any $(x, y) \in F(Y \times_X Y)$, we have $x = F(p_1)(x, y) = F(p_2)(x, y) = y$. Since $F(Y) \xhookrightarrow{\Delta} F(Y \times_X$ we conclude that $F(p_1)$ is bijective. By $(G6)$ p_1 is an isomorphism.

"$\Leftarrow$" Now suppose p_1 is an isomorphism. We can easily see that p_2 is also an isomorphism by $(G4)$ and $(G6)$. From the following commutative diagram

$$\begin{tikzcd}
Y \arrow[dr, dashed, "\Delta"] \arrow[drr, bend left, "\mathrm{id}_Y"] \arrow[ddr, bend right, "\mathrm{id}_Y"'] & & \\
& Y \times_X Y \arrow[r, "p_1"] \arrow[d, "p_2"] & Y \arrow[d, "f"] \\
& Y \arrow[r, "f"'] & X
\end{tikzcd}$$

we can get $\Delta = p_1^{-1} = p_2^{-1}$. Suppose we have morphisms $Z \overset{h}{\underset{g}{\rightrightarrows}} Y$ with $fh = fg$. Then there exists a unique $\phi : Z \to Y \times_X Y$ such that the following diagram

$$\begin{tikzcd}
Z \arrow[dr, dashed, "\phi"] \arrow[drr, bend left, "h"] \arrow[ddr, bend right, "g"'] & & \\
& Y \times_X Y \arrow[r, shift left, "p_1"] \arrow[d, shift left, "p_2"] & Y \arrow[l, shift left, "\Delta"] \arrow[d, "f"] \\
& Y \arrow[u, shift left, "\Delta"] \arrow[r, "f"'] & X
\end{tikzcd}$$

is commutative. Then $g = p_2\phi = p_2(\Delta h) = (p_2\Delta)h = h$, i.e. f is a monomorphism.

(b) We can immediately get (b) from (a).

$\square$

Lemma 2.2.3. *Let $\mathcal{C}$ be a category, $Y \xrightarrow{f} X \xleftarrow{f'} Y'$ morphisms in $\mathcal{C}$, and suppose that the fibre product $Y \times_X Y'$ exists. If $Y \xrightarrow{f} X$ is a monomorphism, then so is $Y \times_X Y' \xrightarrow{p_2} Y'$.*

Proof. For any object Z in $\mathcal{C}$ and morphisms $Z \underset{h}{\overset{g}{\rightrightarrows}} Y \times_X Y'$ with $p_2 h = p_2 g$ then $f' p_2 h = f' p_2 g$. Since $f' p_2 = f p_1$ we have $f p_1 h = f p_1 g$ hence $p_1 h = p_1 g$. Thus we can obtain the following commutative diagram

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

The universal property of the fibre product implies $g = h$ hence p_2 is a monomorphism. Actually the composition $Y \times_X Y' \xrightarrow{p_2} Y' \xrightarrow{f'} X$ is also a monomorphism. $\square$

Definition 2.2.1. A category $\mathcal{C}$ is *artinian* if any decreasing sequence

$$X_1 \xleftarrow[j_1]{} X_2 \xleftarrow[j_2]{} X_3 \xleftarrow[j_3]{} \cdots$$

of monomorphisms in $\mathcal{C}$ is stationary, i.e., there exists a positive integer n_0 such that the j_n are isomorphisms for all $n \geq n_0$.

Lemma 2.2.4. *A Galois category is artinian.*

This lemma follows from $(G6)$ and Lemma 2.2.2. Note that each $F(X_i)$ is finite.

Let A be an object of $\mathcal{C}$ and $a \in F(A)$. For each object X there is a map $\mathrm{Mor}_{\mathcal{C}}(A, X) \to F(X)$ induced by a sending $f \in \mathrm{Mor}_{\mathcal{C}}(A, X)$ to $F(f)(a)$.

Definition 2.2.2. Let $\mathcal{C}$ be a category and F a set-valued covariant functor on $\mathcal{C}$. We say that F is *pro-representable* if $\exists$ a directed set I, a projective system $(A_i,\ \varphi_{ij})_{i \in I}$ of objects in $\mathcal{C}$ and elements $a_i \in F(A_i)$ such that

(i) $a_i = F(\varphi_{ij})(a_j)$ for $j \geq i$.

(ii) For any $X \in \mathrm{Ob}(\mathcal{C})$, the natural map

$$\varinjlim_{i \in I} \mathrm{Mor}_{\mathcal{C}}(A_i, X) \longrightarrow F(X)$$

induced by a_i is bijective.

In addition, if the φ_{ij} are epimorphisms of $\mathcal{C}$, we say that F is *strictly pro-representable.*

Let $\mathcal{C}$ be a essentially small Galois category with a fundamental functor F. Without loss of generality we assume $\mathcal{C}$ is small. Now we consider the set J of pairs (X, a) with X an object of $\mathcal{C}$ and $a \in F(X)$. We define a relation on J as follows:

$$(X, a) \geq (X', a') \iff \exists f \in \mathrm{Mor}_{\mathcal{C}}(X, X') \text{ such that } a' = F(f)(a)$$

which is also denoted by $(X, a) \underset{f}{\geq} (X', a')$ when f is given. This relation is reflexive and transitive since $(X, a) \underset{\mathrm{id}_X}{\geq} (X, a)$ and $(X, a) \underset{f}{\geq} (Y, b)$, $(Y, b) \underset{g}{\geq} (Z, c) \Rightarrow (X, a) \underset{gf}{\geq} (Z, c)$. Actually it may not be antisymmetric so it is not a partial order on J. But we will see later that it is a partial order on a subset of J. We say that a pair (X, a) is *minimal* in J if for any $(Y, b) \underset{j}{\geq} (X, a)$ with j a monomorphism in $\mathcal{C}$, then j is necessarily an isomorphism. Let I denote the subset of J consisting of all minimal pairs of J. Next lemma tells us minimal pairs exist in J.

Lemma 2.2.5. *For any $(Y, b) \in J$, there exists a pair $(X, a) \in I$ such that $(X, a) \geq (Y, b)$.*

This lemma follows from the fact that $\mathcal{C}$ is artinian (Lemma 2.2.4).

Lemma 2.2.6. *If $(X, a) \in I$ and $(Y, b) \in J$ then a $u \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$ such that $(X, a) \underset{u}{\geq} (Y, b)$ is uniquely determined.*

Proof. Suppose we have $u_1, u_2 \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$ such that $(X, a) \underset{u_1}{\geq} (Y, b)$ and $(X, a) \underset{u_2}{\geq} (Y, b)$. Then by $(G1)$ and Lemma 2.2.1 the equalizer of (E, e) of $X \underset{u_2}{\overset{u_1}{\rightrightarrows}} Y$ exists.

$$E \overset{e}{\hookrightarrow} X \underset{u_2}{\overset{u_1}{\rightrightarrows}} Y \qquad \text{and} \qquad F(E) \overset{F(e)}{\hookrightarrow} F(X) \underset{F(u_2)}{\overset{F(u_1)}{\rightrightarrows}} F(Y)$$

By Remark 2.2.1, $(F(E), F(e))$ is the equalizer of $(F(u_1), F(u_2))$. Since $F(u_1)(a) = F(u_2)(a) = b$ we have $a \in F(E)$, i.e., $(E, a) \underset{e}{\geq} (X, a)$ with e a monomorphism. Hence e is an isomorphism, i.e., $u_1 = u_2$. $\square$

Thanks to this lemma, we can show that the relation $\geq$ is antisymmetric on the set of isomorphism classes of elements in I hence is a partial order on I.

Lemma 2.2.7. *$(I, \geq)$ is a directed partially ordered set.*

Proof. It is enough to show that the relation $\geq$ is antisymmetric on I and I is directed.

- Antisymmetry.

Suppose we have both $(X, a) \underset{f}{\geq} (Y, b)$ and $(Y, b) \underset{g}{\geq} (X, a)$ in I, then Lemma 2.2.6 implies $gf = \mathrm{id}_X$ and $fg = \mathrm{id}_Y$, so that (X, a) and (Y, b) are the same up to isomorphism.

- I is directed.

In fact, if (X, a), $(X', a') \in I$. By $(G4)$ and Remark 2.2.1 we get the following diagrams:

$$\begin{tikzcd} X \times X' \arrow[r, "p'"] \arrow[d, "p"'] & X' \\ X & \end{tikzcd} \qquad \text{and} \qquad \begin{tikzcd} F(X \times X') = F(X) \times F(X') \arrow[r, "F(p')"] \arrow[d, "F(p)"'] & F(X') \\ F(X) & \end{tikzcd}$$

where p and p' are the natural projections. Since $(a, a') \in F(X \times X')$ with $F(p)(a, a') = a$ and $F(p')(a, a') = a'$ we have $(X \times X', (a, a')) \underset{p}{\geq} (X, a)$ and $(X \times X', (a, a')) \underset{p'}{\geq} (X', a')$. In fact, $(X \times X', (a, a'))$ may not be in I. Thanks to Lemma 2.2.5, there exists an $(Y, b) \in I$ such that $(Y, b) \geq (X \times X', (a, a'))$ hence $(Y, b) \geq (X, a)$ and $(Y, b) \geq (X', a')$. I is directed. $\square$

Lemma 2.2.8. *If $(X, a) \in I$, $(Y, b) \in J$ and $u \in \mathrm{Mor}_{\mathcal{C}}(Y, X)$ with $(Y, b) \underset{u}{\geq} (X, a)$, then u is an epimorphism.*

Proof. In fact, by $(G3)$ we have a factorization of u

$$\begin{tikzcd} Y \arrow[rr, "u"] \arrow[dr, "u_1"'] & & X_1 \amalg X_0 = X \\ & X_1 \arrow[ur, hook, "u_2"'] & \end{tikzcd}$$

with u_1 an epimorphism and u_2 an monomorphism. Then $a = F(u)(b) = F(u_2 u_1)(b) = F(u_2)F(u_1)(b)$ implies $a \in X_1$. This means that $(X_1, a) \underset{u_2}{\geq} (X, a)$ hence $X_1 \cong X \;\Rightarrow\; u$ is an epimorphism. $\square$

Lemma 2.2.9. *The fundamental functor F of a Galois category $\mathcal{C}$ is strictly pro-representable.*

Proof. Denote I as in Lemma 2.2.5. An element $i \in I$ is a minimal pair (A_i, a_i) in J. If $(A_i, a_i) \geq (A_j, a_j)$ we denote the unique morphism by φ_{ij} such that $(A_i, a_i) \underset{\varphi_{ij}}{\geq} (A_j, a_j)$. We write $i \underset{\varphi_{ij}}{\geq} j$ instead of $(A_i, a_i) \underset{\varphi_{ij}}{\geq} (A_j, a_j)$ for convenience. Then $(A_i, \varphi_{ij})_{i\in I}$ is a projective system. If $i \underset{\varphi_{ij}}{\geq} j$ in I then the diagram of induced maps

$$\begin{tikzcd}
\mathrm{Mor}_{\mathcal{C}}(A_j, X) \arrow[d] \arrow[dr] & \\
& F(X) \\
\mathrm{Mor}_{\mathcal{C}}(A_i, X) \arrow[ur] &
\end{tikzcd}$$

is commutative for any X, so there is a map $\varinjlim_{i\in I} \mathrm{Mor}_{\mathcal{C}}(A_i, X) \longrightarrow F(X)$. By Lemma 2.2.5 this is onto; it is injective since $\mathrm{Mor}_{\mathcal{C}}(A_i, X) \to F(X)$: $u \mapsto F(u)(a_i)$ is injective for each i by Lemma 2.2.6. From Lemma 2.2.8 the φ_{ij} are epimorphisms. It thus follows that F is strictly pro-representable. $\square$

Next, we will discuss what conditions should an object A satisfies such that the pair (A, a) with some $a \in F(A)$ is in I.

Definition 2.2.3. Let $\mathcal{C}$ be a category with initial object. An object X is called *connected* if it has precisely two distinct subobjects, namely $\mathbf{0}_{\mathcal{C}} \to X$, and $\mathrm{id}_X : X \to X$. Equivalently, an object X is connected in $\mathcal{C} \Leftrightarrow X \neq X_1 \amalg X_2$ in $\mathcal{C}$ with $X_1,\ X_2 \neq \mathbf{0}_{\mathcal{C}}$.

Let $\mathcal{C}$ be a Galois category with fundamental functor F. Using the notations above, we have:

Lemma 2.2.10. (1) *$(X, a) \in I \;\Leftrightarrow\; X$ is connected in $\mathcal{C}$.*

(2) *If X is connected in $\mathcal{C}$, then any $u \in \mathrm{Mor}_{\mathcal{C}}(X, X)$ is an automorphism.*

(3) *For any object X, $\mathrm{Aut}(X)$ acts on $F(X)$ by $u \cdot a = F(u)(a)$, $\forall\ u \in \mathrm{Aut}(X)$, $\ \forall\ a \in F(X)$. If X is connected, then for any $a \in F(X)$ the map $\theta_a : \mathrm{Aut}(X) \to F(X)$ defined by $u \mapsto F(u)(a) = u \cdot a$ is injective.*

Proof. (1) "$\Rightarrow$" Let $(X, a) \in I$. Suppose $X \neq X_1 \amalg X_2$ in $\mathcal{C}$ with $X_1,\ X_2 \neq \mathbf{0}_{\mathcal{C}}$ and that $(X, a) \in J$. Then by $(G5)$ $a \in F(X) = F(X_1) \amalg F(X_2)$, say, $a \in F(X_1)$. Let $X_1 \overset{j}{\hookrightarrow} X$ be the morphism such that $(X_1, a) \underset{j}{\geq} (X, a)$ with a monomorphism j which is not an isomorphism, which is a contradiction with $(X, a) \in I$.

"$\Leftarrow$" Now let X be connected and $(X, a) \in J$. Suppose we have $(Y, b) \underset{j}{\geq} (X, a)$ with j a monomorphism. By $(G3)$ we have a factorization:

$$
\begin{tikzcd}
Y \arrow[rr, "j"] \arrow[dr, "j_1"'] & & X_1 \amalg X_0 = X \\
& X_1 \arrow[ur, hook, "j_2"'] &
\end{tikzcd}
$$

with j_1 an epimorphism and j_2 a monomorphism. As j is a monomorphism, so is j_1 thus j_1 is an isomorphism. Then j is an isomorphism since X is connected.

(2) As X is connected, by similar argument in the proof of "$\Leftarrow$" part in (1) we have u is an epimorphism. By $(G5)$, $F(u) : F(X) \to F(X)$ is onto thus is bijective. Then by $(G6)$ $u \in \operatorname{Aut}(X)$.

(3) Let $u_1, u_2 \in \operatorname{Aut}(X)$ such that $F(u_1)(a) = \theta_a(u_1) = \theta_a(u_2) = F(u_2)(a)$, i.e., $a \in E'$, where E' is the equalizer of (u_1, u_2). By Remark 2.2.1 $E' = F(E)$ where E is the equalizer of (u_1, u_2). Then $(E, a) \underset{e}{\geq} (X, a)$ with a monomorphism e. By (1), $(X, a) \in I$ thus e is an isomorphism, i.e., $u_1 = u_2$. $\square$

Let X be a connected object. Then $|\operatorname{Aut}(X)| \leq |\operatorname{Mor}_{\mathcal{C}}(X, X)| \leq |F(X)|$, where the second inequality follows from Lemma 2.2.6. So $\operatorname{Aut}(X)$ is finite.

Definition 2.2.4. A connected object X is *Galois* if for any $a \in F(X)$, the map $\theta_a : \operatorname{Aut}(X) \to F(X)$ defined by $u \mapsto F(u)(a) = u \cdot a$ is bijective.

Note that X is a Galois object $\Leftrightarrow$ the action of $\operatorname{Aut}(X)$ on $F(X)$ is transitive

$\Leftrightarrow$ the quotient $X/\operatorname{Aut}(X)$ is $\mathbf{1}_{\mathcal{C}}$ $\Leftrightarrow$ $F(X)/\operatorname{Aut}(X)$ is a singleton.

The action is also free by Lemma 2.2.10.

Lemma 2.2.11. *Put $\Lambda = \{(X,a) \in I \mid A$ is Galois $\}$. Then Λ is cofinal in I. In other words, for any $(Y,b) \in I$, there is a Galois object X in $\mathcal{C}$, $a \in F(X)$ and a $u \in \mathrm{Mor}_{\mathcal{C}}(X,Y)$ such that $(X,a) \underset{u}{\geq} (Y,b)$.*

Proof. Let $\{(A_i, \varphi_{ij})\}_{i\in I}$ be a projective system as in Lemma 2.2.9 such that

$$\varinjlim_{i\in I} \mathrm{Mor}_{\mathcal{C}}(A_i, X) \xrightarrow{\sim} F(X).$$

Let $F(Y) = \{b_1, b_2, \ldots, b_n\}$. By Lemma 2.2.5, for each $1 \leq j \leq r$, $\exists\ (A_{i_j}, a_{i_j}) \in I$ such that $(A_{i_j}, a_{i_j}) \geq (Y, b_j)$. Taking N large enough we obtain a pair $(A_N, a_N) \in I$ such that $(A_N, a_N) \geq (Y, b_j)$ for all $1 \leq j \leq r$. This implies $\{u \cdot a_N = F(u)(a_N) \mid u \in \mathrm{Mor}_{\mathcal{C}}(A_N, Y)\} = F(Y)$. Then there exists $\alpha : A_N \to Y^r = Y \times \cdots \times Y$ such that

$$A_N \xrightarrow{\alpha} Y^r = Y \times \cdots \times Y \xrightarrow{p_j} Y \qquad \text{and}$$

$$(A_N, a_N) \underset{\alpha}{\geq} (Y^r, (b_1, \ldots, b_n)) \underset{p_j}{\geq} (Y, b_j)$$

where p_j is the j^{th} projection $Y^r \to Y$. Then the elements $(p_j\alpha) \cdot a_N$ are precisely $b_1, \ldots, b_n$. By $(G3)$ we obtain a factorization:

$$\begin{tikzcd} A_N \arrow[rr, "\alpha"] \arrow[dr, "\alpha_1"'] & & Y^r \\ & X \arrow[ur, hook, "\beta"'] & \end{tikzcd}$$

with α_1 an epimorphism and β a monomorphism. We claim that X is Galois.

$(*)$ X is connected.

Suppose $X = X_1 \amalg X_2$, $X_1, X_2 \neq \mathbf{0}_{\mathcal{C}}$. Then $a = F(\alpha_1)(a_N) \in F(X) = F(X_1) \amalg F(X_2)$, say, $a \in F(X_1)$. By Lemma 2.2.5 there is $(A_M, a_M) \in I$ such that $(A_M, a_M) \underset{\varphi_{ij}}{\geq} (A_N, a_N)$, $(A_M, a_M) \underset{\alpha'}{\geq} (X_1, a) \underset{\beta'}{\geq} (X, a)$ with morphisms in the following diagram.

$$\begin{tikzcd} A_N \arrow[rr, "\alpha_1"] & & X = X_1 \amalg X_2 \\ & X_1 \arrow[ur, hook, "\beta'"'] & \\ A_M \arrow[uu, "\varphi_{ij}"] \arrow[ur, "\alpha'"'] & & \end{tikzcd}$$

Since $F(\alpha_1 \circ \varphi_{ij})(a_M) = F(\alpha_1)F(\varphi_{ij})(a_M) = F(\alpha_1)(a_N) = a$, we have $(A_M, a_M) \underset{\alpha_1 \circ \varphi_{ij}}{\geq} (X, a)$. Then by Lemma 2.2.6, we have $\beta' \circ \alpha' = \alpha_1 \circ \varphi_{ij}$, i.e., the diagram above commutes. This, together with Lemma 2.2.8 imply $\beta' \circ \alpha'$ is an epimorphism, which is impossible. Then X is connected and by Lemma 2.2.10 the map $\mathrm{Aut}(X) \to F(X)$ is injective.

($**$) Let $a = F(\alpha_1)(a_N)$. We will prove that the map $\theta_a : \mathrm{Aut}(X) \to F(X)$: $u \mapsto u \cdot a$ is surjective.

Let $a' \in F(X)$. By taking N large enough we may assume that $(A_N, a_N) \underset{\alpha_1}{\geq} (X, a)$ and $(A_N, a_N) \underset{\alpha_1'}{\geq} (X, a')$. Then $(p_j\beta) \cdot a = (p_j\alpha) \cdot a_N$, $1 \leq j \leq r$ give us all the distinct elements of $F(Y)$. Hence the morphisms $p_j\beta$ are all distinct. By Lemma 2.2.8 α_1' is an epimorphism thus $p_j\beta\alpha_1'$ are distinct morphisms. Then $(p_j\beta) \cdot a'$ are precisely all elements of $F(Y)$.

Now we have $(p_j\beta) \cdot a = (p_j\alpha) \cdot a_N = b_j$. Let $b_{\rho(j)} = (p_j\beta) \cdot a'$. We obtain a permutation ρ' of set $\{1, 2, \ldots, r\}$ which will induce an automorphism ρ on Y^r such that the following diagram

$$\begin{tikzcd} & X \arrow[r, hook, "\beta"] & Y^r \arrow[dd, "\rho"] \\ A_N \arrow[ur, "\alpha_1"] \arrow[dr, "\alpha_1'"'] & & \\ & X \arrow[r, hook, "\beta"] & Y^r \end{tikzcd}$$

commutes. This gives us two expression of $\alpha : A_N \to Y^r$ as the composite of an epimorphism and a monomorphism. Since such factorization is unique up to isomorphism, we then obtain an isomorphism $v \in \mathrm{Aut}(X)$ such that $\alpha_1' = v\alpha_1$. It follows θ_a is a surjection and X is Galois with $(X, a) \underset{p_j\beta}{\geq} (Y, b_j)$ for any $b_j \in F(Y)$. □

2.2.2 Proof of the Theorem

Let $\mathcal{C}$ be a small Galois category with fundamental functor F. We may assume now that F is strictly pro-represented by a projective system $(A_i, \varphi_{ij})_{i\in\Lambda}$ with each A_i Galois object of $\mathcal{C}$.

Let $\pi_i = \mathrm{Aut}(A_i)$ and θ_i be the bijection $\pi_i \to F(A_i)$, $u \mapsto u \cdot a_i$ where $a_i \in A_i$ and $(A_i, a_i) \in \Lambda$.

For $j \geq i$ we define $\psi_{ij} : \pi_j \to \pi_i$ as the composite map

$$\pi_j \xrightarrow{\theta_j} F(A_j) \xrightarrow{F(\varphi_{ij})} F(A_i) \xrightarrow{\theta_i^{-1}} \pi_i.$$

Then for any $u \in \pi_j$ we have

$$\psi_{ij}(u) \cdot a_i = \theta_i(\psi_{ij}(u)) = F(\varphi_{ij})\theta_j(u) = F(\varphi_{ij})(u \cdot a_j) = F(\varphi_{ij})F(u)(a_j) = (\varphi_{ij}u) \cdot a_j.$$

This implies $(A_j, a_j) \underset{\psi_{ij}(u)\varphi_{ij}}{\geq} (A_i, b_i)$ and $(A_j, a_j) \underset{\varphi_{ij}u}{\geq} (A_i, b_i)$, where $b_i = \psi_{ij}(u) \cdot a_i = (\varphi_{ij}u) \cdot a_j$. By lemma 2.2.6, $\psi_{ij}(u)\varphi_{ij} = \varphi_{ij}u$, i.e., the following diagram commutes.

$$\begin{tikzcd}
A_i \arrow[r, "\psi_{ij}(u)"] & A_i \\
A_j \arrow[u, "\varphi_{ij}"] \arrow[r, "u"'] & A_j \arrow[u, "\varphi_{ij}"']
\end{tikzcd}$$

It follows that ψ_{ij} are group homomorphisms. Since each φ_{ij} is epimorphism and θ_i, θ_j are bijective, by $(G5)$ each ψ_{ij} is surjective. Now we obtain a projective system of finite groups $(\pi_i, \psi_{ij})_{i\in\Lambda}$. Let

$$\pi = \varprojlim_{i\in\Lambda} \pi_i = \{(u_i)_{i\in\Lambda} \in \prod_{i\in\Lambda} \pi_i \ : \ \psi_{ij}(u_j) = u_i \text{ for all } j \geq i\}.$$

Then π is a profinite group by giving $\prod_{i\in\Lambda} \pi_i$ the product topology and π the relative topology.

For any object X of $\mathcal{C}$, the group π_i acts on $\mathrm{Mor}_{\mathcal{C}}(A_i, X)$ to the left by $(\sigma, f) \mapsto f\sigma^{-1}$. For any $\sigma \in \pi_i$, $f \in \mathrm{Mor}_{\mathcal{C}}(A_i, X)$ and for $j \geq i$, let $\widetilde{\sigma}$ be an element in π_j with $\psi_{ij}(\widetilde{\sigma}) = \sigma$. We have $\widetilde{\sigma} \cdot (f\varphi_{ij}) = f\varphi_{ij}\widetilde{\sigma}^{-1}$ and $(f\sigma^{-1}) \circ \varphi_{ij} = f \circ (\psi_{ij}(\widetilde{\sigma}^{-1})\varphi_{ij}) = f\varphi_{ij}\widetilde{\sigma}^{-1}$. This implies the group action we defined above is compatible with the map $\pi_j \xrightarrow{\psi_{ij}} \pi_i$ and $\mathrm{Mor}_{\mathcal{C}}(A_i, X) \xrightarrow{\widetilde{\varphi_{ij}}} \mathrm{Mor}_{\mathcal{C}}(A_j, X)$, where $\widetilde{\varphi_{ij}}$ is the map induced by φ_{ij} sending $f \in \mathrm{Mor}_{\mathcal{C}}(A_i, X)$ to $f \circ \varphi_{ij} \in \mathrm{Mor}_{\mathcal{C}}(A_j, X)$. Thus the actions of π_i on $\mathrm{Mor}_{\mathcal{C}}(A_i, X)$ induce a continuous π-action on the set $\varinjlim_{i\in\Lambda} \mathrm{Mor}_{\mathcal{C}}(A_i, X) \xrightarrow{\sim} F(X)$. Since $F(X)$ is finite, the action of π on $F(X)$ is determined by the action of some π_i on $F(X)$. If $f : X \to Y$ is a morphism in $\mathcal{C}$ then the induced map $\varinjlim_{i\in\Lambda} \mathrm{Mor}_{\mathcal{C}}(A_i, X) \to \varinjlim_{i\in\Lambda} \mathrm{Mor}_{\mathcal{C}}(A_i, Y)$ is a morphism of π-sets since the action comes from π_i for some sufficiently large i. We have the following commutative diagram.

$$\begin{tikzcd}
\varinjlim_{i\in\Lambda} \mathrm{Mor}_{\mathcal{C}}(A_i, X) \arrow[d] & \mathrm{Mor}_{\mathcal{C}}(A_i, X) \arrow[l] \arrow[r] \arrow[d] & F(X) \arrow[d, "F(f)"] \\
\varinjlim_{i\in\Lambda} \mathrm{Mor}_{\mathcal{C}}(A_i, Y) & \mathrm{Mor}_{\mathcal{C}}(A_i, Y) \arrow[l] \arrow[r] & F(Y)
\arrow[from=1-1, to=1-3, bend left]
\arrow[from=2-1, to=2-3, bend right]
\end{tikzcd}$$

Thus $F(f)$ is a morphism of π-sets.

Let us recall basic facts about the pro-category $\mathrm{Pro}\,\mathcal{C}$. Informally speaking, an object of $\mathrm{Pro}\,\mathcal{C}$ (called a pro-object of $\mathcal{C}$) is a projective system $\widetilde{P} = (P_i)_{i\in I'}$ in $\mathcal{C}$. If $\widetilde{P}$, $\widetilde{P'} = (P'_j)_{j\in J'}$ are pro-objects of $\mathcal{C}$, we define

$$\mathrm{Mor}_{\mathrm{Pro}\,\mathcal{C}}(\widetilde{P}, \widetilde{P'}) = \varprojlim_{j\in J'} \varinjlim_{i\in I'} \mathrm{Mor}_{\mathcal{C}}(P_i, P'_j).$$

An object of $\mathcal{C}$ will be considered as an object of $\mathrm{Pro}\,\mathcal{C}$ in a natural way. In this notation, a pro-representable functor on $\mathcal{C}$ can be seen as a functor "represented" by a pro-object of $\mathcal{C}$. Let $\mathcal{C}$ be a small Galois category with fundamental functor F. For any object X in $\mathcal{C}$ we have:

$$F(X) \xleftarrow{\sim} \varinjlim_{i\in\Lambda} \mathrm{Mor}_{\mathcal{C}}(A_i, X) \simeq \mathrm{Mor}_{\mathrm{Pro}\,\mathcal{C}}(\widetilde{A}, X)$$

where $\widetilde{A}$ is the pro-object $(A_i)_{i\in\Lambda}$ of $\mathcal{C}$. Hence each element of $F(X)$ can be seen as a $\mathrm{Pro}\,\mathcal{C}$-morphism $\widetilde{A} \to X$. Since A_i is a Galois object in $\mathcal{C}$, we have $\mathrm{Mor}_{\mathrm{Pro}\,\mathcal{C}}(\widetilde{A}, A_i) \cong F(A_i) \cong \mathrm{Mor}_{\mathcal{C}}(A_i, A_i) = \mathrm{Aut}(A_i) = \pi_i$ and then

$$\begin{aligned}
\pi = \varprojlim_{i\in\Lambda} \pi_i &= \varprojlim_{i\in\Lambda} \mathrm{Mor}_{\mathcal{C}}(A_i, A_i) \\
&= \varprojlim_{i\in\Lambda} \mathrm{Mor}_{\mathrm{Pro}\,\mathcal{C}}(\widetilde{A}, A_i) \\
&= \mathrm{Mor}_{\mathrm{Pro}\,\mathcal{C}}(\widetilde{A}, \widetilde{A}) = \mathrm{Aut}(\widetilde{A}).
\end{aligned}$$

Next we will give a description of connected objects in π-**Sets**.

Lemma 2.2.12. *An object E of π-**Sets** is connected if and only if the action of π on E is transitive.*

This lemma follows from the Definition 2.2.3 immediately.

If we write $H(X)$ for the set $F(X)$ equipped with the π-action and $H(f) = F(f)$ for a morphism f in $\mathcal{C}$. Then H is a functor $\mathcal{C} \to \pi$-**Sets** that composed with the forgetful functor π-**Sets** $\to$ **Sets** yields F (we shall see later that this H is the same as we defined in section 2.1.6). Then we obtain an equivalence of categories.

Lemma 2.2.13. *The functor $H : \mathcal{C} \to \pi$-**Sets** is an equivalence of categories.*

Proof. Claim 1 : H is essentially surjective.

Let E be any π-set. By $(G2)$ and $(G5)$ we may assume that E is connected in the category π-**Sets**, i.e., π acts transitively on E. Fix an element $e \in E$, the map $\pi \to E$ defined by $\sigma \mapsto \sigma \cdot e$ is a surjection. As E is finite, this map will factor through π_i for some $i \in \Lambda$,

$$\begin{tikzcd} \pi \arrow[rr] \arrow[dr, "f_i"'] & & E \\ & \pi_i \arrow[ur] & \end{tikzcd}$$

where $f_i : \pi \to \pi_i$ is the natural projection and the map $\pi_i \to E$ is defined by the group action on e. Obviously this holds for each $j \geq i$. Let $H_i \subseteq \pi_i$ be the isotropy group of e in π_i, i.e., $H_i = \{\sigma \in \pi_i : \sigma \cdot e = e\}$. There is a natural action of π on π_i/H_i induced by left multiplication. We define a map $\Gamma : \pi_i/H_i \to E$ by $\sigma H_i \mapsto \sigma \cdot e$. Obviously Γ is a bijective. For any $\tau \in \pi$ we have $\Gamma(\tau \cdot \sigma H_i) = \Gamma(f_i(\tau)\sigma H_i) = (f_i(\tau)\sigma) \cdot e = f_i(\tau) \cdot (\sigma \cdot e) = \tau \cdot (\sigma \cdot e) = \tau \cdot \Gamma(\sigma H_i)$. So Γ is an isomorphism in π-**Sets**.

We then let $\widehat{E_i} := A_i/H_i$ be the quotient described in section 2.1.4. By $(G2)$, $\widehat{E_i}$ is an object in $\mathcal{C}$ and by $(G5)$, $F(\widehat{E_i}) = F(A_i)/H_i \cong \pi_i/H_i \cong E$ as π-sets. If $j \geq i$ and $H_j \subseteq \pi_j$ is the isotropy group of e in π_j, the group homomorphism $\psi_{ij} : \pi_j \to \pi_i$ induces a map $\pi_j/H_j \to \pi_i/H_i$ by $\sigma H_j \mapsto \psi_{ij}(\sigma)H_i$. Since the following diagram

$$\begin{tikzcd} \pi_j \arrow[rr, "\psi_{ij}"] \arrow[dr] & & \pi_i \arrow[dl] \\ & E & \end{tikzcd}$$

commutes, i.e., $\psi_{ij}(H_j) \subseteq H_i$ then the map $\pi_j/H_j \to \pi_i/H_i$ is well defined. Notice that we have the following two diagram.

$$\begin{tikzcd} A_j \arrow[r, "\varphi_{ij}"] \arrow[d, "\rho_j"'] & A_i \arrow[d, "\rho_i"] \\ A_j/H_j & A_i/H_i \end{tikzcd} \qquad \begin{tikzcd} A_i \arrow[r, "\psi_{ij}(\sigma)"] & A_i \\ A_j \arrow[u, "\varphi_{ij}"] \arrow[r, "\sigma"'] & A_j \arrow[u, "\varphi_{ij}"'] \end{tikzcd}$$

with the second one commutative. For any $\sigma \in H_j$ thus $\rho_j\sigma = \rho_j$ and $\psi_{ij}(\sigma) \in H_i$. We have

$$(\rho_i\varphi_{ij})\sigma = \rho_i(\varphi_{ij}\sigma) = \rho_i\psi_{ij}(\sigma)\varphi_{ij} = \rho_i\varphi_{ij}.$$

Then there exists a unique morphism $\mu_{ij} : A_j/H_j \to A_i/H_i$ such that $\rho_i\varphi_{ij} = \mu_{ij}\rho_j$. Looking at the images of $\widehat{E_j} := A_j/H_j$ and $\widehat{E_i} := A_i/H_i$ under F we have a commutative diagram.

$$\begin{tikzcd} F(A_j/H_j) \arrow[r, "F(\mu_{ij})"] \arrow[d, "\sim"] & F(A_i/H_i) \arrow[d, "\sim"] \\ E \arrow[r, "\sim"] & E \end{tikzcd}$$

Thus $F(\mu_{ij})$ is an isomorphism of π-sets. By $(G6)$, $\widehat{E_j} \cong \widehat{E_i}$. This means that the object $\widehat{E_i}$ such that $F(\widehat{E_i}) \cong E$ is independent of the choice of i hence we denote it by $\widehat{E}$ and denote the isomorphism $F(\widehat{E}) \xrightarrow{\sim} E$ by γ_E.

Now consider the map $H : \mathrm{Mor}_{\mathcal{C}}(X, Y) \to \mathrm{Mor}_{\pi\text{-}\mathbf{Sets}}(F(X), F(Y))$ by $f \mapsto F(f)$.

Claim 2 : H is injective.

Let $f, g \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$ with $F(f) = F(g)$. Let (E, e) be the equalizer of $X \underset{g}{\overset{f}{\rightrightarrows}} Y$. By $(G4)$ and Remark 2.2.1, $(F(E), F(e))$ is the equalizer of $F(X) \underset{F(g)}{\overset{F(f)}{\rightrightarrows}} F(Y)$. Since $F(f) = F(g)$ $F(e)$ is an isomorphism thus e is an isomorphism by $(G6)$. This implies $f = g$.

Claim 3 : H is surjective.

As in *Claim 1* we can assume X is connected. Fix an element $a \in F(X)$. By Lemma 2.2.11 there exists $(A_N, a_N) \in \Lambda$ and $f \in \mathrm{Mor}_{\mathcal{C}}(A_N, X)$ such that $(A_N, a_N) \underset{f}{\geq} (X, a)$. Actually, take N large enough we may also assume that the map $\mathrm{Mor}_{\mathcal{C}}(A_N, X) \to F(X)$, $g \mapsto F(g)(a)$ is bijective. By $(G3)$ and the connectedness of X the map $F(f) : F(A_N) \to F(X)$ is surjective. Take any $f' \in \mathrm{Mor}_{\mathcal{C}}(A_N, X)$ then there exists an $a'_N \in F(A_N)$ such that $F(f)(a'_N) = F(f')(a_N)$. As A_N is a

Galois object of $\mathcal{C}$, π_N acts transitively on $F(A_N)$. Thus we can find a $\sigma \in \pi_N$ such that $\sigma \cdot a_N = a'_N$, i.e., $F(\sigma)(a_N) = a'_N$. Then $F(f)(F(\sigma)(a_N)) = F(f\sigma)(a_N) = F(f')(a_N)$. By Lemma 2.2.6, $f\sigma = f'$, i.e., $f = \sigma \cdot f'$. This means the action of π_N on $\mathrm{Mor}_{\mathcal{C}}(A_N, X)$ is transitive. Hence we obtain an isomorphism of π-sets $F(X) \cong \pi_N/G$ where G is the isotropy group of f in π_N. Since $F(X)$ is finite, the map $\pi \to F(X)$, $\sigma \mapsto \sigma \cdot a$ can be factored through some π_M.

$$\begin{tikzcd}
\pi \arrow[rr] \arrow[dr, "f_M"'] & & F(X) \\
& \pi_M \arrow[ur] &
\end{tikzcd}$$

By taking M large enough (namely $M \geq N$) we may assume that π_M acts transitively on $\mathrm{Mor}_{\mathcal{C}}(A_M, X)$—

Since f_M is surjective, π acts on $F(X)$ transitively thus $F(X)$ is connected in π-**Sets**.

For any $\alpha : F(X) \to F(Y)$, let $b = \alpha(a)$. The Pro $\mathcal{C}$-morphism $b : \widetilde{A} \to Y$ can be factored through some A_i as follows

$$\begin{tikzcd}
\widetilde{A} \arrow[rr, "b"] \arrow[dr, "g_i"'] & & Y \\
& A_i \arrow[ur, "b_k"'] &
\end{tikzcd}$$

for some $b_k \in F(Y)$. Take i large enough such that $\mathrm{Mor}_{\mathcal{C}}(A_i, Y) \xrightarrow{\sim} F(Y)$ and $(A_i, a_i) \underset{f_k}{\geq} (Y, b_k)$ for all $b_k \in F(Y)$. Recall that $\forall\, \sigma \in \pi_i$, $\sigma \cdot f_k = f_k \circ \sigma^{-1}$ and $\sigma \cdot b_k = F(f_k \circ \sigma^{-1})(a_i) = F(f_k)F(\sigma)^{-1}(a_i)$. Let H_i, H'_i, H''_i be the isotropy group of a, a_i and b_i in π_i, respectively. Then we have $H_i \subseteq H'_i \subseteq H''_i$. The map $b_k : A_i \to Y$ can be factored through $A_i/H_i \cong \widehat{F(X)}$ for i sufficiently large and the following diagram

$$\begin{tikzcd}
\widetilde{A} \arrow[r, "b"] \arrow[d, "g_i"'] & Y \\
A_i \arrow[r] \arrow[ur, "b_k"] & A_i/H_i \arrow[u, "u"']
\end{tikzcd}$$

is commutative. Similarly, by taking i large enough, we have $v : A_i/H_i \cong \widehat{F(X)} \to X$ such that the diagram

$$\begin{tikzcd}
\widetilde{A} \arrow[r, "a"] \arrow[d, "f_i"'] & X \\
A_i \arrow[r] \arrow[ur, "a_i"] & A_i/H_i \arrow[u, "v"']
\end{tikzcd}$$

commutes. Then $F(v) \circ \gamma_{F(X)}^{-1} = \mathrm{id}_X$, which implies $F(v)$ is an isomorphism. Thus v is an isomorphism by $(G6)$. So we have a composite

$$X \xrightarrow{v^{-1}} \widehat{F(X)} \xrightarrow{u} Y.$$

We complete the proof of this lemma. $\square$

Next lemma gives a concrete description of the automorphism group of the forgetful functor from **π-Sets** to **Sets**.

Lemma 2.2.14. *Let π be a profinite group and F the forgetful functor from π-**Sets** to **Sets**. Then* $\mathrm{Aut}(F) \cong \pi$.

Proof. As π is a profinite group, $\pi \cong \varprojlim_{\pi' \triangleright \pi \text{ open}} \pi/\pi'$, where π' ranging over the open normal subgroups of π. π/π' is automatically a π-set where the action is induced by left multiplication. For any $\sigma \in \mathrm{Aut}(F)$, σ is determined by the bijections $\sigma_X : F(X) \to F(X)$. For any $X \in \mathrm{Ob}(\mathcal{C})$, fix an element $x \in F(X)$. Let $x' = \sigma_X(x)$ and π_x be the isotropy group of x in π. Since π acts on X continuously, π_x is an open normal subgroup of π. Similarly we may assume that X is connected, i.e., π acts transitively on X. Then $\pi/\pi_x \to X$ by $\overline{a} \mapsto a \cdot x$ is an isomorphism as π-sets. We have the following commutative diagram.

$$\begin{tikzcd}
F(\pi/\pi_x) \arrow[r, "\sim"] \arrow[d, "\tau"] & F(X) \arrow[d, "\sigma_x"] \\
F(\pi/\pi_{x'}) \arrow[r, "\sim"] & F(X)
\end{tikzcd}$$

where $\tau : \pi/\pi_x \to \pi/\pi_{x'}$ given by $a\pi_x \mapsto a\pi_{x'}$ is an isomorphism. In fact, for any $a \in \pi$, $x \in X$ we have $a \cdot x = x \Leftrightarrow a \cdot x' = x'$ with $x' = \sigma_X(x)$. Then $\pi_x = \pi_{x'}$ thus each τ gives rise to a map $\sigma_{\pi/\pi_x} : F(\pi/\pi_x) \to F(\pi/\pi_x)$. So σ_X is determined by such $\sigma_{\pi/\pi'}$ with π' ranging over the open normal subgroups of π.

Next we will prove that the map $\Phi : \pi/\pi' \to \mathrm{Aut}_{\pi\text{-}\mathbf{Sets}}(\pi/\pi')$ defined by $a\pi' \mapsto (f_a : b\pi' \mapsto ba^{-1}\pi')$ is a group isomorphism.

- Φ is well defined.

  For $a,\, a' \in \pi$ with $a\pi' = a'\pi'$, thus $aa'^{-1} \in \pi'$, we have

  $$f_a(b\pi') = ba^{-1}\pi' = ba^{-1}aa'^{-1}\pi' = ba'^{-1}\pi' = f_{a'}(b\pi').$$

  Moreover, $f_a(a' \cdot b\pi') = f_a(a'b\pi') = a'ba^{-1}\pi' = a' \cdot f_a(b\pi')$. Then it is easy to see that $f_a \in \mathrm{Aut}_{\pi\textbf{-Sets}}(\pi/\pi')$.

- Clearly Φ is injective and a group homomorphism.

- Φ is surjective.

  $\forall \sigma \in \mathrm{Aut}_{\pi\textbf{-Sets}}(\pi/\pi')$, $\forall a \in \pi$, fix some $b\pi' \in \pi/\pi'$ for some $b \in \pi$, let $\sigma(b\pi') = b'\pi'$ for some $b' \in \pi$ and set $a = b'^{-1}b$. We have $f_a(b\pi') = bb^{-1}b'\pi' = b'\pi'$. For any $d\pi' \in \pi/\pi'$,

  $$\sigma(d\pi') = \sigma(db^{-1}b\pi') = (db^{-1}) \cdot (b'\pi') = da^{-1}\pi' = f_a(d\pi').$$

  Then $\sigma = f_a$.

Similarly we have any set-theoretic map $\pi/\pi' \to \pi/\pi'$ commuting with all π-**Sets**-automorphisms of π/π' is given by left multiplication by some $b\pi' \in \pi/\pi'$. Then $\mathrm{Aut}(F) \cong \varprojlim_{\pi' \triangleright \pi \text{ open}} \mathrm{Aut}(\pi/\pi') \cong \varprojlim_{\pi' \triangleright \pi \text{ open}} \pi/\pi' = \pi$. Hence the functor $H : \pi\textbf{-Sets} \to \mathrm{Aut}(F)\textbf{-Sets}$ defined in section 2.1.6 is the identity functor. $\square$

Now we prove the main theorem in this chapter, Theorem 2.2.1.

Proof of Theorem 2.2.1. We first prove (b). Let π be any profinite group and $H : \mathcal{C} \to \pi\textbf{-Sets}$ be an equivalence such that composed with the forgetful functor $F_1 : \pi\textbf{-Sets} \to \textbf{Sets}$ it yields F. As H is a equivalence we have $\mathrm{Aut}(F) \cong \mathrm{Aut}(F_1)$. By Lemma 2.2.14, $\pi \cong \mathrm{Aut}(F_1) \cong \mathrm{Aut}(F)$. This shows (b) and (a) follows from (b) immediately.

Now suppose (A, a), $(A, a') \in \Lambda$, $\mathrm{Aut}(A)$ acts on $F(A)$ transitively. Then there exists a $u \in \mathrm{Aut}(A)$ such that $u(a) = a'$ thus $(A, a) = (A, a')$ in Λ. This means all pairs (A, a) $in \Lambda$ with the same A are isomorphic, we may replace Λ by a subset Λ_1 containing exactly one pair (A, a) for each Galois object A. Now we prove (c). Let F' be a second fundamental functor on $\mathcal{C}$. F, F' are pro-represented by pro-objects $\widetilde{A}$, $\widetilde{B}$, respectively. Then we have

$$F = \mathrm{Mor}_{\mathrm{Pro}\,\mathcal{C}}(\widetilde{A}, -) = \varinjlim_{i \in \Lambda_1} \mathrm{Mor}_{\mathcal{C}}(A_i, -) \quad \text{and} F' = \mathrm{Mor}_{\mathrm{Pro}\,\mathcal{C}}(\widetilde{B}, -) = \varinjlim_{j \in \Lambda_2} \mathrm{Mor}_{\mathcal{C}}(B_j, -)$$

where Λ_1, Λ_2 are subsets of Λ containing exactly one pair (A, a) for each Galois object A. It suffices to prove that $\widetilde{A} \cong \widetilde{B}$ in $\mathrm{Pro}\,\mathcal{C}$. We denote the canonical morphism $A_j \to A_i$ (resp. $B_j \to B_i$) by p_{ij} (resp. q_{ij}) for $j \geq i$, and the map $\widetilde{A} \to A_i$ (resp. $\widetilde{B} \to B_j$) by p_i (resp. q_j). Let $a_i \in F(A_i)$ (resp. $b_j \in F(B_j)$) be the element such that $(A_i, a_i)\ in \Lambda_1$ (resp. $(B_j, b_j)\ in \Lambda_2$). For any $j \in \Lambda_2$ consider the $\mathrm{Pro}\,\mathcal{C}$-morphism $b_j : \widetilde{A} \to B_j$. Since $b_l = q_{lj} \circ b_j$ they induce a $\mathrm{Pro}\,\mathcal{C}$-morphism $b : \widetilde{A} \to \widetilde{B}$ such that the following diagram commutes.

$$\begin{tikzcd}
\widetilde{A} \arrow[rr, "b"] \arrow[dr, "b_j"'] & & \widetilde{B} \arrow[dl, "q_j"] \\
& B_j &
\end{tikzcd}$$

For any $b_j : \widetilde{A} \to B_j$, there exists $i_j \in \Lambda_1$ such that $(A_{i_j}, a_{i_j}) \geq (B_j, b_j)$ and the following diagram

$$\begin{tikzcd}
\widetilde{A} \arrow[r, "b"] \arrow[d, "p_{i_j}"'] \arrow[dr, "b_j"] & \widetilde{B} \arrow[d, "q_j"] \\
A_{i_j} \arrow[r] & B_j
\end{tikzcd}$$

is commutative. Similarly, we can get a commutative diagram in other direction $\widetilde{B} \to \widetilde{A}$. Then $\widetilde{A} \cong \widetilde{B}$ in $\mathrm{Pro}\,\mathcal{C}$. This implies $F \cong F'$ and proves (c). (d) follows from (b) and (c).

This completes the proof the Theorem 2.2.1.

Chapter 3

Finite étale coverings

This chapter contains some basic properties for finite étale coverings. In the first two sections, we introduce the affine information needed for finite étale morphisms. Throughout the first two sections, let A be a ring (commutative with identity).

3.1 Projective modules and projective algebras

Definition 3.1.1. Let $0 \to M_0 \to M_1 \to M_2 \to 0$ be a short exact sequence of modules over a ring A. The sequence is said to *split* if there is an isomorphism $M_1 \xrightarrow{\sim} M_0 \oplus M_2$ of A-modules for which the diagram

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

(with the obvious maps in the bottom row) is commutative.

Proposition 3.1.1. *Let $0 \to M_0 \xrightarrow{f} M_1 \xrightarrow{f'} M_2 \to 0$ be a short exact sequence of modules over a ring A. The following three statements are equivalent:*

(i) the sequence $0 \to M_0 \to M_1 \to M_2 \to 0$ splits;

(ii) there is an A-linear map $h : M_1 \to M_0$ such that $h \circ f = id_{M_0}$;

(iii) there is an A-linear map $h' : M_2 \to M_1$ such that $f' \circ h' = id_{M_2}$.

Proof. $(i) \Rightarrow (ii)$: Suppose the sequence splits. By definition there is an isomorphism $\varphi : M_1 \xrightarrow{\sim} M_0 \oplus M_2$ of A-modules such that the following diagram

$$\begin{tikzcd} M_0 \arrow[r, "f"] \arrow[d, "\mathrm{id}"] & M_1 \arrow[d, "\varphi"] & \\ M_0 \arrow[r, "g_1"] & M_0 \oplus M_2 \arrow[r, "p_1"] & M_0 \end{tikzcd}$$

commutes, where g_1 is the natural inclusion and p_1 is the projection with $p_1 \circ g_1 = \mathrm{id}_{M_0}$. Let h be the composite

$$M_1 \xrightarrow{\varphi} M_0 \oplus M_2 \xrightarrow{p_1} M_0 .$$

Then $h \circ f = (p_1\varphi)f = p_1 g_1 \mathrm{id}_{M_0} = \mathrm{id}_{M_0}$ as required.

$(ii) \Rightarrow (iii)$: Suppose we have an A-linear map $h : M_1 \to M_0$ with $hf = \mathrm{id}_{M_0}$,

$$\begin{tikzcd} 0 \arrow[r] & M_0 \arrow[r, "f"] & M_1 \arrow[r, "f'"] \arrow[l, bend left, "h"] & M_2 \arrow[r] & 0. \end{tikzcd}$$

For any $x \in M_2$, since f' is surjective, there exists a $y \in M_1$, such that $f'(y) = x$. Then we define a map

$$h' : M_2 \longrightarrow M_1, \quad x \mapsto y - f \circ h(y).$$

- h' is well defined. Suppose we have $y, y' \in M_1$ with $f'(y) = f'(y') = x$. Thus $y - y' \in \mathrm{Ker}(f') = \mathrm{Im}(f)$, i.e., there is a $z \in M_0$ such that $f(z) = y - y'$. Then $z = h \circ f(z) = h(y - y')$ and $y - y' = f(z) = f(h(y - y'))$. This implies $h'(y) = y - fh(y) = y' - fh(y') = h'(y')$, i.e., h' is well defined.

- h' is A-linear since f, h are A-linear.

- $\forall x \in M_2$, we have

$$f' \circ h'(x) = f'(y - fh(y)) = f'(y) - (f'f)(h(y)) = f'(y) = x$$

  since $f'f = 0$, i.e., $f' \circ h' = \mathrm{id}_{M_2}$.

$(iii) \Rightarrow (i)$: Suppose we have an A-linear map $h' : M_2 \to M_1$ with $f'h' = \mathrm{id}_{M_2}$,

$$\begin{tikzcd} 0 \arrow[r] & M_0 \arrow[r, "f"] & M_1 \arrow[r, "f'"] & M_2 \arrow[r] \arrow[l, bend left, "h'"] & 0. \end{tikzcd}$$

For any $x \in M_1$, consider the difference $x - h'f'(x)$ in M_1. We have

$$f'(x - h'f'(x)) = f'(x) - (f'h')(f'(x)) = f'(x) - f'(x) = 0,$$

i.e., $x - h'f'(x) \in \mathrm{Ker}(f') = \mathrm{Im}(f)$. Since f is injective, there exists a unique $\widehat{x} \in M_0$ such that $f(\widehat{x}) = x - h'f'(x)$. We define a map

$$\psi : M_1 \longrightarrow M_0 \oplus M_2, \quad x \mapsto (\widehat{x}, f'(x)).$$

- It is easy to see that ψ is a homomorphism of A-modules.
- ψ is injective. Suppose we have $\widehat{x} = 0$ and $f'(x) = 0$ for some $x \in M_1$. Then $x - h'f'(x) = f(\widehat{x}) = 0$, i.e., $x = h'f'(x) = h'(0) = 0$.
- ψ is surjective. For any $(y, z) \in M_0 \oplus M_2$ with $y \in M_0$ and $z \in M_2$, let $x = f(y) + h'(z)$. Then we have

  $$f'(x) = f'f(y) + f'h'(z) = 0 + z = z, \text{ and} f(y) = x - h'(z) = x - h'(f'(x)).$$

  Remember that $\widehat{x}$ is the unique element in M_0 with $f(\widehat{y}x) = x - h'f'(x)$, which implies $\widehat{x} = y$. Thus $\psi(x) = (y, z)$.
- For any $y \in M_0$, since $f'f = 0$ then $f(y) = f(y) - h'(f'f)(y) = f(y) - (h'f')(f(y))$, which implies $\widehat{f(y)} = y$. We have the following commutative diagrams.

$$\begin{tikzcd} M_0 \arrow[r, "f"] \arrow[d, "\mathrm{id}"'] & M_1 \arrow[d, "\varphi", "\sim"'] \\ M_0 \arrow[r] & M_0 \oplus M_2 \end{tikzcd} \qquad \text{by} \qquad \begin{tikzcd} y \arrow[r, mapsto] \arrow[d, mapsto] & f(y) \arrow[d, mapsto] \\ y \arrow[r, mapsto] & (y, 0) = (\widehat{f(y)}, f'f(y)) \end{tikzcd}$$

and

$$\begin{tikzcd} M_1 \arrow[r, "f'"] \arrow[d, "\varphi"', "\sim"] & M_2 \arrow[d, "\mathrm{id}"] \\ M_0 \oplus M_2 \arrow[r] & M_2 \end{tikzcd} \qquad \text{by} \qquad \begin{tikzcd} x \arrow[r, mapsto] \arrow[d, mapsto] & f'(x) \arrow[d, mapsto] \\ (\widehat{x}, f'(x)) \arrow[r, mapsto] & f'(x) \end{tikzcd}$$

These prove that the sequence $0 \to M_0 \to M_1 \to M_2 \to 0$ splits. $\square$

Lemma 3.1.1. *Let M be an A-module, $(P_i)_{i\in I}$ be a collection of A-modules and $P = \bigoplus_{i\in I} P_i$. Then (1) $\mathrm{Hom}_A(P, M) \cong \prod_{i\in I} \mathrm{Hom}_A(P_i, M)$; (2) $P \otimes_A M \cong \bigoplus_{i\in I}(P_i \otimes_A M)$.*

Proof. Let φ_j be the natural map $P_j \to P$, $p_j \mapsto (p_i)_{i\in I}$ where $p_i = p_j$ if $i = j$ and $p_i = 0$ if $i \neq j$. Obviously, $\varphi_j \in \mathrm{Hom}_A(P_j, P)$. We first prove (1). For any $f \in \mathrm{Hom}_A(P, M)$, we have $f \circ \varphi_j \in \mathrm{Hom}_A(P_j, M)$. We then define a map

$$\psi : \mathrm{Hom}_A(P, M) \longrightarrow \prod_{i\in I} \mathrm{Hom}_A(P_i, M), \quad f \mapsto (f \circ \varphi_i)_{i\in I}.$$

- It is easy to see that ψ is a homomorphism of A-modules.

- ψ is injective. Suppose we have an $f \in \mathrm{Hom}_A(P, M)$ such that $f \circ \varphi_i = 0$ for any $i \in I$. Take any $x = (p_i)_{i\in I} \in P = \bigoplus_{i\in I} P_i$, thus p_i is zero for all but finitely many i. Suppose $p_{i_1}, p_{i_2}, \ldots, p_{i_n}$ are all the nonzero components. Then $x = \varphi_{i_1}(p_{i_1}) + \varphi_{i_2}(p_{i_2}) + \cdots + \varphi_{i_n}(p_{i_n})$. This implies $f(x) = f\varphi_{i_1}(p_{i_1}) + f\varphi_{i_2}(p_{i_2}) + \cdots + f\varphi_{i_n}(p_{i_n}) = 0$. Since x is arbitrary, $f = 0$.

- ψ is surjective. For any $(f_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_A(P_i, M)$, we define

  $$f : P \longrightarrow M, \quad x = (p_i)_{i\in I} \mapsto \sum_{j\in J} f_j(p_j),$$

  where J is a finite subset of I such that $x = \sum_{j\in J} \varphi_j(p_j)$. It is easy to show that $f \in \mathrm{Hom}_A(P, M)$ and $\psi(f) = (f_i)_{i\in I}$.

So ψ is an isomorphism, which proves (1).

For (2), we define $f_i : P_i \times M \to P \otimes_A M$ by $(p_i, m) \mapsto \varphi_i(p_i) \otimes m$. f_i is A-bilinear for each $i \in I$. By the universal property of the tensor product, there exists a unique A-linear map $g_i : P_i \otimes_A M \to P \otimes_A M$ such that the following diagram

$$\begin{tikzcd}
P_i \times M \arrow[r] \arrow[d, "f_i"'] & P_i \otimes_A M \arrow[dl, dashed, "g_i"'] \\
P \otimes_A M &
\end{tikzcd}$$

commutes. These maps will induce a map

$$\begin{aligned} g: \bigoplus_{i\in I}(P_i \otimes_A M) &\longrightarrow P \otimes_A M, \\ (p_i \otimes m_i)_{i\in I} &\longmapsto \sum_{i\in I} g_i(p_i \otimes m_i) = \sum_{i\in I}(\varphi_i(p_i) \otimes m_i). \end{aligned}$$

This map is well defined since the sum on the right hand side is taken over only finitely many nonzero elements.

We also have an A-bilinear map $h' : P \times M \to \bigoplus_{i\in I}(P_i \otimes_A M)$, $((p_i)_{i\in I}, m) \mapsto (p_i \otimes m)_{i\in I}$. It induces an A-linear map $h : P \otimes_A M \to \bigoplus_{i\in I}(P_i \otimes_A M)$ such that the following diagram

$$\begin{tikzcd} P \times M \arrow[r] \arrow[d, "h'"'] & P \otimes_A M \arrow[dl, dashed, "h"'] \\ \bigoplus_{i\in I}(P_i \otimes_A M) & \end{tikzcd}$$

is commutative. Then it is easy to check that $g \circ h = \mathrm{id}_{P\otimes_A M}$ and $h \circ g = \mathrm{id}_{\bigoplus_{i\in I}(P_i \otimes_A M)}$, which shows (2). $\square$

Remark 3.1.1. Let $(P_i)_{i\in I}$ be a collection of A-modules and $P = \bigoplus_{i\in I} P_i$. By the above lemma, we can easily show that the functor $\mathrm{Hom}_A(P, -)$ (resp. $- \otimes_A P$) is exact if and only if each $\mathrm{Hom}_A(P_i, -)$ (resp. $- \otimes_A P_i$) is exact.

Proposition 3.1.2. *For any A-module P the following four assertions are equivalent:*

(i) The functor $\mathrm{Hom}_A(P, -)$ *is exact, i.e., if*

$$0 \longrightarrow M_0 \xrightarrow{\varphi} M_1 \xrightarrow{\psi} M_2 \longrightarrow 0$$

is a short exact sequence of A-modules, then

$$0 \longrightarrow \mathrm{Hom}_A(P, M_0) \xrightarrow{\varphi'} \mathrm{Hom}_A(P, M_1) \xrightarrow{\psi'} \mathrm{Hom}_A(P, M_2) \longrightarrow 0$$

is also a short exact sequence, where φ', ψ' are natural homomorphisms induced by φ and ψ, respectively.

(ii) For every surjective A-homomorphism $f : M \to N$ and every A-homomorphism $g : P \to N$ there exists an A-homomorphism $h : P \to M$ such that $g = fh$:

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

(iii) Every exact sequence $0 \to L \to M \to P \to 0$ splits.

(iv) P is a direct summand of a free A-module.

Proof. $(i) \Rightarrow (ii)$ is trivial.

$(ii) \Rightarrow (iii)$: Let $N = P$ and $g = \mathrm{id}_P$ in (ii), then (iii) follows immediately using Proposition 3.1.1.

$(iii) \Rightarrow (iv)$: Remember that every A-module P is a quotient of a free A-module and apply (iii).

$(iv) \Rightarrow (i)$: Suppose P is a direct summand of a free A-module. By Remark 3.1.1, it suffices to show that $\mathrm{Hom}_A(A, -)$ is exact. This is obvious since $\mathrm{Hom}_A(A, M) \cong M$ for every A-module M. $\square$

Definition 3.1.2. An A-module P is called *projective* if it satisfies any of the equivalent conditions of Proposition 3.1.2.

Corollary 3.1.1. *Free modules are projective. A finitely generated module is projective if and only if it is a direct summand of a finitely generated free module.*

Proof. The first assertion is obvious. The second statement follows from Proposition 3.1.2 (iii). $\square$

Remark 3.1.2. Recall that an A-module P is called *flat* if the functor $- \otimes_A P$ is exact. Free modules are flat hence projective modules are flat by Remark 3.1.1.

Example 3.1.1. (1) If $A = K$ is a field, then every A-module is free and hence projective.

(2) If A is a principal ideal domain, a projective A-module is free.

(3) Suppose $A \cong A_1 \times A_2$ for rings A_1 and A_2. Then each A_i is a projective A-module. If the A_i are nonzero they are not free. Let P be any A-module. There is an isomorphism $P \cong P_1 \times P_2$, where $P_i = e_i P_i$ is an A_i module with $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Moreover, P is projective over A if and only if each P_i is projective over A_i.

Lemma 3.1.2. *Let M, N and P be A-modules and P is flat. For any $f \in \operatorname{Hom}_A(M, N)$, we have:*

(1) $\operatorname{Ker}(f \otimes id_P) \cong \operatorname{Ker}(f) \otimes_A P$ *and*

(2) $\operatorname{Coker}(f \otimes id_P) \cong \operatorname{Coker}(f) \otimes_A P$ *hence* $\operatorname{Im}(f \otimes id_P) \cong \operatorname{Im}(f) \otimes_A P$.

Proof. (1) We have an exact sequence $0 \to \operatorname{Ker}(f) \to M \to N$. Since P is flat, the sequence $0 \to \operatorname{Ker}(f) \otimes_A P \to M \otimes_A P \to N \otimes_A P$ is also exact. For any $x \in \operatorname{Ker}(f)$ and any $p \in P$, $(f \otimes \mathrm{id}_P)(x \otimes p) = f(x) \otimes p = 0$. This implies $\operatorname{Ker}(f) \otimes_A P \subseteq \operatorname{Ker}(f \otimes \mathrm{id}_P)$. We have the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, equal] & 0 \arrow[r] \arrow[d, equal] & \operatorname{Ker}(f) \otimes_A P \arrow[r] \arrow[d, hook] & M \otimes_A P \arrow[r, "f\otimes\mathrm{id}_P"] \arrow[d, "\cong"', "\mathrm{id}"] & N \otimes_A P \arrow[d, "\cong"', "\mathrm{id}"] \\
0 \arrow[r] & 0 \arrow[r] & \operatorname{Ker}(f \otimes \mathrm{id}_P) \arrow[r] & M \otimes_A P \arrow[r, "f\otimes\mathrm{id}_P"] & N \otimes_A P
\end{tikzcd}$$

with each row exact. By five lemma, $\operatorname{Ker}(f) \otimes_A P \cong \operatorname{Ker}(f \otimes \mathrm{id}_P)$.

(2) We start with another exact sequence $M \to N \to \operatorname{Coker}(f) \to 0$. Since P is flat, the sequence $M \otimes_A P \to N \otimes_A P \to \operatorname{Coker}(f) \otimes_A P \to 0$ is also exact. There is a natural A-bilinear map $\operatorname{Coker}(f) \times P \to \operatorname{Coker}(f \otimes \mathrm{id}_P)$ with $(\overline{x}, p) \mapsto \overline{x \otimes p}$. This induces an A-linear map $\phi : \operatorname{Coker}(f) \otimes_A P \to \operatorname{Coker}(f \otimes \mathrm{id}_P)$ and we obtain the following commutative diagram

$$\begin{tikzcd}
M \otimes_A P \arrow[r, "f\otimes\mathrm{id}_P"] \arrow[d, "\cong"', "\mathrm{id}"] & N \otimes_A P \arrow[r] \arrow[d, "\cong"', "\mathrm{id}"] & \operatorname{Coker}(f) \otimes_A P \arrow[r] \arrow[d, "\phi"] & 0 \arrow[r] \arrow[d, equal] & 0 \arrow[d, equal] \\
M \otimes_A P \arrow[r, "f\otimes\mathrm{id}_P"] & N \otimes_A P \arrow[r] & \operatorname{Coker}(f \otimes \mathrm{id}_P) \arrow[r] & 0 \arrow[r] & 0
\end{tikzcd}$$

with each row exact. By five lemma, $\operatorname{Coker}(f \otimes \mathrm{id}_P) \cong \operatorname{Coker}(f) \otimes_A P$ and thus $\operatorname{Im}(f \otimes \mathrm{id}_P) \cong \operatorname{Im}(f) \otimes_A P$. ☐

Proposition 3.1.3. *Let A be a local ring with maximal ideal $\mathfrak{m}$ and P a finitely generated A-module. Then P is projective if and only if it is free.*

Proof. The "if" part is obvious. For the "only if" part, since P is a finitely generated A-module, $P \otimes_A A/\mathfrak{m}$ is a finite dimensional vector space. Take $x_1, x_2, \ldots, x_n \in P$ such that $\{x_1 \otimes 1, x_2 \otimes 1, \ldots, x_n \otimes 1\}$ is a basis of $P \otimes_A A/\mathfrak{m}$. Let $f : A^n \to P$ be the map sending the i-th basis to x_i. Then $f \otimes \mathrm{id}_{A/\mathfrak{m}} : A^n \otimes_A A/\mathfrak{m} \to P \otimes_A A/\mathfrak{m}$ is an isomorphism since it is a linear map between two vector spaces sending basis to basis. Then $M = \mathrm{Coker}(f)$ is finitely generated and $M/\mathfrak{m}M \cong M \otimes_A A/\mathfrak{m} = \mathrm{Coker}(f) \otimes_A A/\mathfrak{m} \cong \mathrm{Coker}(f \otimes \mathrm{id}_{A/\mathfrak{m}}) = 0$, i.e., $M = \mathfrak{m}M$. Nakayama's lemma implies $M = 0$, so f is surjective. Now we get a short exact sequence of A-modules:

$$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow A^n \longrightarrow P \longrightarrow 0.$$

P is projective $\Rightarrow A^n \cong P \oplus \mathrm{Ker}(f) \Rightarrow \mathrm{Ker}(f)$ is finitely generated. Since $\mathrm{Ker}(f)/\mathfrak{m}\,\mathrm{Ker}(f) \cong \mathrm{Ker}(f) \otimes_A A/\mathfrak{m} \cong \mathrm{Ker}(f \otimes \mathrm{id}_{A/\mathfrak{m}}) = 0$. By Nakayama's lemma $\mathrm{Ker}(f) = 0$, i.e. f is injective thus an isomorphism. So P is free. $\square$

Next, we will see some local characterization of projective modules. Recall that for any $f \in A$, $A_f = S^{-1}A$ where $S = \{f^n : n \geq 0\}$ and $M_f = S^{-1}M = M \otimes_A A_f$ for an A-module M. We say that M is *finitely presented* if there is an exact sequence $A^m \to A^n \to M \to 0$ of A-modules with $m, n < \infty$.

Lemma 3.1.3. *Let M, N be A-modules, with M finitely presented and let $S \subset A$ be a multiplicatively closed subset. Then $S^{-1}\,\mathrm{Hom}_A(M, N) \cong \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$ as $S^{-1}A$-modules.*

Proof. The natural map $\varphi : S^{-1}\,\mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$ is given by $\frac{f}{t} \mapsto (f_t : \frac{m}{s} \mapsto \frac{f(m)}{st})$ for any $f \in \mathrm{Hom}_A(M, N)$, $m \in M$ and $s, t \in S$. f_t is $S^{-1}A$-linear because

$$\begin{aligned} f_t(\frac{a}{b}\frac{m_1}{t_1} + \frac{m_2}{t_2}) &= f_t(\frac{am_1t_2 + bt_1m_2}{bt_1t_2}) = \frac{f(am_1t_2 + bt_1m_2)}{tbt_1t_2} \\ &= \frac{af(m_1t_2) + f(bt_1m_2)}{tbt_1t_2} = \frac{a}{b}\frac{t_2f(m_1)}{tt_1t_2} + \frac{bt_1f(m_2)}{tbt_1t_2} \end{aligned}$$

$$= \frac{a}{b} f_t(\frac{m_1}{t_1}) + f_t(\frac{m_2}{t_2}),$$

for any $a \in A$, $m_1, m_2 \in M$ and $b, t_1, t_2 \in S$. It is easy to see that φ is well-defined. We claim that φ is an isomorphism. This is clear if $M = A$ since the following diagram is commutative,

$$\begin{tikzcd} S^{-1}N \arrow[r, "\sim"] \arrow[d, equal] & S^{-1}\operatorname{Hom}_A(A,N) \arrow[d, "\varphi"] \\ S^{-1}N \arrow[r, "\sim"] & \operatorname{Hom}_{S^{-1}A}(S^{-1}A, S^{-1}N) \end{tikzcd} \quad \text{by} \quad \begin{tikzcd} \frac{y}{t} \arrow[r, mapsto] \arrow[d, equal] & \frac{(1\mapsto y)}{t} \arrow[d, mapsto] \\ \frac{y}{t} \arrow[r, mapsto] & (\frac{1}{1} \mapsto \frac{y}{t}) \end{tikzcd}$$

where $(1 \mapsto y)$ denotes the map in $\operatorname{Hom}_A(A, N)$ uniquely determined by sending the identity of A to y. Similarly, taking direct sums we get a commutative diagram

$$\begin{tikzcd} S^{-1}\operatorname{Hom}_A(A^n,N) \arrow[r, "\sim"] \arrow[d, "\varphi"'] & \bigoplus_{i=1}^{n} S^{-1}\operatorname{Hom}_A(A,N) \arrow[d] \\ \operatorname{Hom}_{S^{-1}A}(S^{-1}A^n, S^{-1}N) \arrow[r, "\sim"] & \bigoplus_{i=1}^{n} \operatorname{Hom}_{S^{-1}A}(S^{-1}A, S^{-1}N) \end{tikzcd}$$

by

$$\begin{tikzcd} \frac{y}{t} \arrow[r, mapsto] \arrow[d, mapsto] & \left(\frac{(1\mapsto f(e_1))}{t}, \ldots, \frac{(1\mapsto f(e_n))}{t}\right) \arrow[d, mapsto] \\ \left(f_t : \frac{e_i}{1} \mapsto \frac{f(e_i)}{t}\right) \arrow[r, mapsto] & \left(\frac{1}{1} \mapsto \frac{f(e_1)}{t}, \ldots, \frac{f(e_n)}{t}\right) \end{tikzcd}$$

where $e_i = (0, \ldots, 1, \ldots, 0)$ has a 1 in the i-th component and zeros elsewhere with e_i's forming a free A-basis for A^n. Hence φ is also an isomorphism if $M \cong A^n$ for some $n < \infty$. For general M, since M is finitely presented, we have

$$\begin{aligned} & A^m \xrightarrow{h} A^n \xrightarrow{g} M \to 0 \text{ is exact with } m, n < \infty, \\ \Rightarrow\ & 0 \to \operatorname{Hom}_A(M,N) \to \operatorname{Hom}_A(A^n,N) \to \operatorname{Hom}_A(A^m,N) \text{ is exact} \\ & (\operatorname{Hom}_A(-,N) \text{ is left exact}), \\ \Rightarrow\ & 0 \to S^{-1}\operatorname{Hom}_A(M,N) \to S^{-1}\operatorname{Hom}_A(A^n,N) \to S^{-1}\operatorname{Hom}_A(A^m,N) \text{ is exact} \\ & (S^{-1} \text{ is flat}). \end{aligned}$$

Similarly, we have an exact sequence

$$0 \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}A^n, S^{-1}N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}A^m, S^{-1}N)$$

and the following diagram

$$\begin{tikzcd}
0 \arrow[r] & S^{-1}\operatorname{Hom}_A(M,N) \arrow[r] \arrow[d, "\varphi"'] & S^{-1}\operatorname{Hom}_A(A^n,N) \arrow[r] \arrow[d, "\cong"'] & S^{-1}\operatorname{Hom}_A(A^m,N) \arrow[d, "\cong"'] \\
0 \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N) \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^n,S^{-1}N) \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^m,S^{-1}N)
\end{tikzcd}$$

with both rows exact. The first square is commutative by

$$\begin{tikzcd}
\frac{f}{t} \arrow[r, mapsto] \arrow[d, mapsto] & \frac{f\circ g}{t} \arrow[d, mapsto] \\
\left(f_t : \frac{m}{t'} \mapsto \frac{f(m)}{tt'}\right) \arrow[dr, mapsto] & \left((f\circ g)_t : \frac{x}{t'} \mapsto \frac{fg(x)}{tt'}\right) \arrow[d, equal] \\
& \left(\frac{x}{t'} \mapsto f_t(\frac{g(x)}{t'}) = \frac{fg(x)}{tt'}\right)
\end{tikzcd}$$

and the second square is commutative in similar way. Hence $S^{-1}\operatorname{Hom}_A(M,N) \cong \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N$ by five lemma. $\square$

Lemma 3.1.4. *Let $(f_i)_{i\in I}$ be a collection of elements of A with $\sum_{i\in I} Af_i = A$ and M an A-module.*

(a) If $M_{f_i} = 0$ for all $i \in I$ then $M = 0$.

(b) If M_{f_i} is a finitely generated A_{f_i}-module for each $i \in I$ then M is finitely generated.

Proof. (a) Let $\mathfrak{m}$ be any maximal ideal of A. Since $\sum_{i\in I} Af_i = A$, the set $\{f_i : i \in I\}$ is not contained in $\mathfrak{m}$. There exists an $i_0 \in I$ such that $f_{i_0} \in A - \mathfrak{m}$. $M_{f_{i_0}} = 0 \Rightarrow M_{\mathfrak{m}} = 0 \Rightarrow M = 0$.

(b) Suppose we have $\sum_{i=1}^n a_i f_i = 1$ for some $a_1, \ldots, a_n \in A$. By assumption, we may take a finite subset of M_{f_i} as generators over A_{f_i}. Moreover, we may take the generators of the form $\frac{m_{i1}}{f_i^N}, \frac{m_{i2}}{f_i^N}, \ldots, \frac{m_{ik}}{f_i^N}$ for each $1 \le i \le n$. Then for any $m \in M$, we can write $\frac{m}{1}$ as $\frac{m}{1} = \frac{\sum_{j=i}^k b_{ij} m_{ij}}{f_i^{N'}}$ in M_{f_i} with $b_{ij} \in A$. Then there is an N'' such that $f_i^{N''} m = \sum_{j=1}^k b'_{ij} m_{ij}$.

$\langle f_1, f_2, \ldots, f_n\rangle = (1) \Rightarrow \langle f_1^{N''}, f_2^{N''}, \ldots, f_n^{N''}\rangle = (1)$, i.e., there exist $a'_1, \ldots, a'_n \in A$ such that $\sum_{i=1}^n a'_i f_i^{N''} = 1$. Hence we have

$$m = m \cdot \sum_{i=1}^n a'_i f_i^{N''} = \sum_{i=1}^n a'_i \sum_{j=1}^k b'_{ij} m_{ij} = \sum_{i=1}^n \sum_{j=1}^k c_{ij} m_{ij}$$

with $c_{ij} \in A$. So M is a finitely generated over A. $\square$

Theorem 3.1.1. *Let P be an A-module. The following are equivalent:*

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

(ii) P is finitely presented and $P_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module for any prime ideal $\mathfrak{p}$ of A.

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

(iv) There is a collection $(f_i)_{i\in I}$ of elements of A with $\sum_{i\in I} Af_i = A$ such that P_{f_i} is a free A_{f_i}-module of finite rank for each $i \in I$.

Proof. $(i) \Rightarrow (ii)$: Let Q be such that $P \oplus Q \cong A^n$ for some $n < \infty$. Then Q is finitely generated thus P is finitely presented. Let $\mathfrak{p}$ be a prime ideal of A and we have $A^n_{\mathfrak{p}} \cong (P \oplus Q)_{\mathfrak{p}} \cong P_{\mathfrak{p}} \oplus Q_{\mathfrak{p}}$, which implies $P_{\mathfrak{p}}$ is finitely generated projective over $A_{P_{\mathfrak{p}}}$. By Proposition 3.1.3 $P_{\mathfrak{p}}$ is free.

$(ii) \Rightarrow (iii)$ because a maximal ideal is prime.

$(iii) \Rightarrow (iv)$: Let $\mathfrak{m}$ be a maximal ideal of A and suppose we have

$$\begin{tikzcd} A^n_{\mathfrak{m}} \arrow[r, bend left, "g", "\sim"'] & P_{\mathfrak{m}} \arrow[l, bend left, "h", "\sim"'] \end{tikzcd}$$

where g, h are isomorphisms inverse to each other. By Lemma 3.1.3, $\mathrm{Hom}_{A_{\mathfrak{m}}}(A^n_{\mathfrak{m}}, P_{\mathfrak{m}}) \cong \Big(\mathrm{Hom}_A(A^n, P)\Big)$ and $\mathrm{Hom}_{A_{\mathfrak{m}}}(P_{\mathfrak{m}}, A^n_{\mathfrak{m}}) \cong \Big(\mathrm{Hom}_A(P, A^n)\Big)_{\mathfrak{m}}$, so $g = \frac{g'}{s}$, $h = \frac{h'}{t}$ for some $g' \in \mathrm{Hom}_A(A^n, P)$, $h' \in \mathrm{Hom}_A(P, A^n)$ and certain $s, t \in A - \mathfrak{m}$. Then we have

$$\frac{\mathrm{id}_P}{1} = \mathrm{id}_{P_{\mathfrak{m}}} = \frac{g'h'}{st} \quad \text{and} \quad \frac{\mathrm{id}_{A^n}}{1} = \mathrm{id}_{A^n_{\mathfrak{m}}} = \frac{h'g'}{st}.$$

Then $\exists u, v \in A - \mathfrak{m}$ such that $g'h'u = (stu)\mathrm{id}_P$ and $h'g'v = (stv)\mathrm{id}_{A^n}$. Let $f_{\mathfrak{m}} = stuv$, $g'' = \frac{(tuv)g'}{f_{\mathfrak{m}}}$ and $h'' = \frac{(suv)h'}{f_{\mathfrak{m}}}$. Then $g'' \in \mathrm{Hom}_{A_{f_{\mathfrak{m}}}}(A^n_{f_{\mathfrak{m}}}, P_{f_{\mathfrak{m}}})$ and $h'' \in \mathrm{Hom}_{A_{f_{\mathfrak{m}}}}(P_{f_{\mathfrak{m}}}, A^n_{f_{\mathfrak{m}}})$. Moreover $g''h'' = \frac{g'h'}{st} = \mathrm{id}_{P_{f_{\mathfrak{m}}}}$ and $h''g'' = \frac{h'g'}{st} = \mathrm{id}_{A^n_{f_{\mathfrak{m}}}}$, i.e., g'', h'' are isomorphisms inverse to each other. So $P_{f_{\mathfrak{m}}}$ is a free $A_{f_{\mathfrak{m}}}$-module of finite rank. Let $\mathfrak{m}$ range over all the maximal ideals of A we then obtain a collection of f's that is not contained in any maximal ideal thus generates A.

$(iv) \Rightarrow (i)$: If we write the identity of A as a linear combination of finite f_i we may assume that I is finite. For any $i \in I$, we may choose an isomorphism $g_i : A_{f_i}^{n_i} \to P_{f_i}$ such that the image of the j-th standard basis $(0, \ldots, \frac{1}{1}, \ldots, 0)$ is of the form $\frac{p_{ij}}{1}$ for $1 \leq j \leq n_i$. Let $g_i' : A^{n_i} \to P$ be the map defined by $(0, \ldots, 1, \ldots, 0) \mapsto p_{ij}$. Then the following diagram

$$\begin{tikzcd} A^{n_i} \arrow[r] \arrow[d, "g_i'"'] & A_{f_i}^{n_i} \arrow[d, "g_i"'] \\ P \arrow[r] & P_{f_i} \end{tikzcd}$$

commutes. These g_i''s induce a map $g : A^{\sum_{i \in I} n_i} \to P$ with $\Big(\operatorname{Coker}(g)\Big)_{f_i} = 0$. By Lemma 3.1.4 g is surjective. Consider the map $g \otimes \mathrm{id}_{A_{f_i}} : A_{f_i}^{\sum_{i \in I} n_i} \to P_{f_i}$. Then $\operatorname{Ker}(g \otimes \mathrm{id}_{A_{f_i}}) \cong A_{f_i}^{\sum_{j \neq i} n_i}$ is finitely generated. Hence $\operatorname{Ker}(g)_{f_i} \cong \operatorname{Ker}(g \otimes \mathrm{id}_{A_{f_i}})$ is finitely generated and so is $\operatorname{Ker}(g)$ by Lemma 3.1.4. This implies P is finitely presented. Apply Lemma 3.1.3 to any surjective map $\varphi' : M \to N$ of A-modules, we have the following commutative diagram

$$\begin{tikzcd} \Big(\operatorname{Hom}_A(P, M)\Big)_{f_i} \arrow[r, "\varphi \otimes \mathrm{id}_{A_{f_i}}"] \arrow[d, "\cong"'] & \Big(\operatorname{Hom}_A(P, N)\Big)_{f_i} \arrow[r] \arrow[d, "\cong"'] & \operatorname{Coker}(\varphi \otimes \mathrm{id}_{A_{f_i}}) \arrow[r] & 0 \\ \operatorname{Hom}_{A_{f_i}}(P_{f_i}, M_{f_i}) \arrow[r] & \operatorname{Hom}_{A_{f_i}}(P_{f_i}, N_{f_i}) & & \end{tikzcd}$$

with the first row exact, where $\varphi : \operatorname{Hom}_A(P, M) \to \operatorname{Hom}_A(P, N)$ is the natural map induced by φ'. Moreover, $\varphi' : M \to N$ is surjective implies the map $M_{f_i} \to N_{f_i}$ induced by φ' is also surjective. Then the map in the second row is surjective since P_{f_i} are free thus projective over A_{f_i}. By five lemma, $\operatorname{Coker}(\varphi \otimes \mathrm{id}_{A_{f_i}}) \cong \Big(\operatorname{Coker}(\varphi)\Big)_{f_i} = 0$ thus φ is surjective. By Proposition 3.1.2 P is projective.

This completes the proof of the theorem. $\square$

Now let P be a finitely generated projective A-module. By Theorem 3.1.1 (ii), the $A_{\mathfrak{p}}$-module $P_{\mathfrak{p}}$ is free for each $\mathfrak{p} \in \operatorname{Spec}(A)$ and we denote the rank of $P_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$ by $\operatorname{rk}_{A_{\mathfrak{p}}}(P_{\mathfrak{p}})$. Then we define the rank function

$$\operatorname{rank}(P) = \operatorname{rank}_A(P) : \operatorname{Spec} A \longrightarrow \mathbb{Z} \quad \text{by} \quad \mathfrak{p} \mapsto \operatorname{rk}_{A_{\mathfrak{p}}}(P_{\mathfrak{p}}).$$

We consider the rank function as a function between topological spaces where $\mathbb{Z}$ is equipped with the discrete topology. Then this function is locally constant thus continuous. Moreover, if $\operatorname{Spec} A$ is connected, i.e., A does not contain any nontrivial idempotents, then the function $\operatorname{rank}(P)$ is constant and may be identified with a nonnegative integer.

Definition 3.1.3. Let P be a finitely generated projective A-module. We say that P is *faithfully projective* if $\operatorname{rank}(P)(\mathfrak{p}) \geq 1$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$.

Proposition 3.1.4. *Let P be a finitely generated projective A-module. The following four statements are equivalent:*

(i) *P is faithfully projective.*

(ii) *The map $A \to \operatorname{End}_{\mathbb{Z}}(P)$ giving the A-module structure is injective.*

(iii) *P is faithful, i.e., an A-module M is zero if and only if $M \otimes_A P = 0$.*

(iv) *P is faithfully flat, i.e., a sequence $M_0 \to M_1 \to M_2$ of A-modules is exact if and only if the induced sequence $M_0 \otimes_A P \to M_1 \otimes_A P \to M_2 \otimes_A P$ is exact.*

Proof. First we prove an equivalent condition of (ii). The map $\phi : A \to \operatorname{End}_{\mathbb{Z}}(P)$ defined by $a \mapsto (f_a : p \mapsto a \cdot p)$ is $\mathbb{Z}$-linear and gives $\operatorname{End}_{\mathbb{Z}}(P)$ the A-module structure. Then we have $\operatorname{Ker}(\phi) = \operatorname{Ann}(P)$. So condition (ii) holds if and only if $\operatorname{Ann}(P) = 0$. Now we start the proof of the proposition.

$(i) \Rightarrow (ii)$: Take any $a \in \operatorname{Ann}(P)$, it suffices to show that $a = 0$. First we claim that $a \in \mathfrak{R}(A)$, which is the Jacobson radical of A. If not, then there is a maximal ideal $\mathfrak{m}$ of A such that $a \in A - \mathfrak{m}$. Then $P_{\mathfrak{m}} = 0$ since $a \in \operatorname{Ann}(P)$, a contradiction with P faithfully projective. Hence $a \in \mathfrak{R}(A)$. For any maximal ideal $\mathfrak{m}$ of A, since $P_{\mathfrak{m}}$ is free over $A_{\mathfrak{m}}$ of rank ≥ 1, there exists $x \in P$ and $t \in A - \mathfrak{m}$ such that $\frac{x}{t} \neq 0$. But $\frac{a}{1} \cdot \frac{x}{t} = 0$, this implies $\frac{a}{1} = 0$ in $A_{\mathfrak{m}}$. Then there exists an $s \in A - \mathfrak{m}$ such that $as = 0$. Letting $\mathfrak{m}$ range over all maximal ideals of A, we obtain a collection of s's that is not contained in any maximal ideal and thus generates A. There exists $r_1, r_2, \ldots, r_n \in A$ such that $\sum_{i=1}^n r_i s_i = 1$ where s_i is obtained as above with $as_i = 0$. Then $a = \sum_{i=1}^n r_i s_i a = 0$.

$(ii) \Rightarrow (iii)$: The "only if" part is obvious. For the "if" part, suppose $M \otimes_A P = 0$. For any maximal ideal $\mathfrak{m}$ of A, since P is finitely generated projective, $P_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module of finite rank. Suppose $P_\mathfrak{m} = A_\mathfrak{m}^n$. Since P is finitely generated, by (ii), we have $P_\mathfrak{m} \neq 0$, thus $n \geq 1$. But $0 = (M \otimes_A P)_\mathfrak{m} \cong M_\mathfrak{m} \otimes_{A_\mathfrak{m}} P_\mathfrak{m} \cong M_\mathfrak{m}^n$, therefore $M_\mathfrak{m} = 0$. Thus $M = 0$.

$(iii) \Rightarrow (iv)$: The "only if" part is clear since a projective module is flat. Conversely, suppose $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ is a sequence of A-modules and the induced sequence $M_0 \otimes_A P \xrightarrow{f \otimes \mathrm{id}_P} M_1 \otimes_A P \xrightarrow{g \otimes \mathrm{id}_P} M_2 \otimes_A P$ is exact. Then $0 = (g \otimes \mathrm{id}_P) \circ (f \otimes \mathrm{id}_P) = (gf \otimes \mathrm{id}_P)$. By (iii), $gf = 0$, i.e., $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$. Let $M = \mathrm{Ker}(g)/\mathrm{Im}(f)$, by Lemma 3.1.2, $M \otimes_A P \cong \mathrm{Ker}(g \otimes \mathrm{id}_P)/\mathrm{Im}(f \otimes \mathrm{id}_P) = 0$. Then $M = 0$, i.e., $M_0 \xrightarrow{f} M_1 \xrightarrow{g} M_2$ is exact.

$(iv) \Rightarrow (i)$: We need to show that $\mathrm{rank}(P)(\mathfrak{p}) \geq 1$ for any prime ideal $\mathfrak{p}$ of A, i.e., $P_\mathfrak{p} \neq 0$. Suppose not, i.e., there is a $\mathfrak{p} \in \operatorname{Spec} A$ such that $P_\mathfrak{p} = 0$. Then the sequence $0 \to P_\mathfrak{p} = P \otimes_A A_\mathfrak{p} \to 0$ is exact. By (iv), $0 \to P_\mathfrak{p} \to 0$ is exact, i.e., $A_\mathfrak{p} = 0$. Hence $0 \in A - \mathfrak{p}$, a contradiction.

This completes the proof. □

Let P be a finitely generated projective A-module and $P^\vee = \mathrm{Hom}_A(P, A)$ denote the dual module of P. For each A-module M there is a natural bilinear map:

$$\phi' : P^\vee \times M \to \mathrm{Hom}_A(P, M) \;\text{ with }\; (f, m) \mapsto (p \mapsto f(p) \cdot m).$$

This induces a homomorphism:

$$\phi : P^\vee \otimes_A M \to \mathrm{Hom}_A(P, M) \;\text{ with }\; f \otimes m \mapsto (p \mapsto f(p) \cdot m).$$

We have the following property:

Proposition 3.1.5. *The map $\phi : P^\vee \otimes_A M \to \mathrm{Hom}_A(P, M)$ with $f \otimes m \mapsto (p \mapsto f(p) \cdot m)$ is an isomorphism.*

Proof. The proof of this proposition is similar to the proof of Proposition 3.1.3. Since we have the following commutative diagram,

$$\begin{tikzcd}
A^\vee \otimes_A M \arrow[r, "\phi"] \arrow[d, "\sim"'] & \mathrm{Hom}_A(A, M) \arrow[dd, "\sim"] \\
A \otimes_A M \arrow[d, "\sim"'] & \\
M \arrow[r, equal] & M
\end{tikzcd}
\quad \text{by} \quad
\begin{tikzcd}
f \otimes m \arrow[r, mapsto] \arrow[d, mapsto] & (a \mapsto f(a) \cdot m) \arrow[dd, mapsto] \\
f(1) \otimes m \arrow[d, mapsto] & \\
f(1) \cdot m \arrow[r, equal] & f(1) \cdot m
\end{tikzcd}$$

ϕ is an isomorphism if $P = A$. Taking direct sums we have that ϕ is an isomorphism if $P \cong A^n$ for some $n < \infty$. For general P, the same conclusion is obtained by passing to direct summands and applying five lemma. $\square$

Proposition 3.1.6. *Let P and P' be finitely generated projective A-modules. Then the A-modules $P \oplus P'$, $P \otimes_A P'$, $\mathrm{Hom}_A(P, P')$ and $P^\vee$ are finitely generated projective and the rank of these modules are given by*

$$\mathrm{rank}(P \oplus P') = \mathrm{rank}(P) + \mathrm{rank}(P'),$$

$$\mathrm{rank}(P \otimes_A P') = \mathrm{rank}(P) \times \mathrm{rank}(P'),$$

$$\mathrm{rank}(\mathrm{Hom}_A(P, P')) = \mathrm{rank}(P) \times \mathrm{rank}(P'),$$

$$\mathrm{rank}(P^\vee) = \mathrm{rank}(P),$$

as functions on $\mathrm{Spec}\, A$*.*

Proof. Let Q and Q' be A-modules such that $P \oplus Q$ and $P' \oplus Q'$ are free A-modules of finite rank. Then

$$(P \oplus Q) \oplus (P' \oplus Q') \cong (P \oplus P') \oplus Q_1,$$

$$(P \oplus Q) \otimes_A (P' \oplus Q') \cong (P \otimes_A P') \oplus Q_2,$$

$$\mathrm{Hom}_A(P \oplus Q, P' \oplus Q') \cong \mathrm{Hom}_A(P, P') \oplus Q_3 \quad \text{and}$$

$$(P \oplus Q)^\vee \cong P^\vee \oplus Q^\vee$$

verify the claim $P \oplus P'$, $P \otimes_A P'$, $\mathrm{Hom}_A(P, P')$ and $P^\vee$ are finitely generated projective over A, respectively. Moreover, for any $\mathfrak{p} \in \operatorname{Spec} A$, we have

$$(P \oplus P')_\mathfrak{p} \cong P_\mathfrak{p} \oplus P'_\mathfrak{p} \cong A_\mathfrak{p}^{\mathrm{rank}(P)(\mathfrak{p})} \oplus A_\mathfrak{p}^{\mathrm{rank}(P')(\mathfrak{p})} \cong A_\mathfrak{p}^{\mathrm{rank}(P)(\mathfrak{p})+\mathrm{rank}(P')(\mathfrak{p})},$$

$$(P \otimes_A P')_\mathfrak{p} \cong P_\mathfrak{p} \otimes_{A_\mathfrak{p}} P'_\mathfrak{p} \cong A_\mathfrak{p}^{\mathrm{rank}(P)(\mathfrak{p})} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}^{\mathrm{rank}(P')(\mathfrak{p})} \cong A_\mathfrak{p}^{\mathrm{rank}(P)(\mathfrak{p})\cdot\mathrm{rank}(P')(\mathfrak{p})},$$

$$\begin{aligned}(\mathrm{Hom}_A(P, P'))_\mathfrak{p} &\cong \mathrm{Hom}_{A_\mathfrak{p}}(P_\mathfrak{p}, P'_\mathfrak{p}) \cong \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}^{\mathrm{rank}(P)(\mathfrak{p})}, A_\mathfrak{p}^{\mathrm{rank}(P')(\mathfrak{p})}) \\ &\cong A_\mathfrak{p}^{\mathrm{rank}(P)(\mathfrak{p})\cdot\mathrm{rank}(P')(\mathfrak{p})} \quad \text{and}\end{aligned}$$

$$(P^\vee)_\mathfrak{p} \cong \mathrm{Hom}_{A_\mathfrak{p}}(P_\mathfrak{p}, A_\mathfrak{p}) \cong \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}^{\mathrm{rank}(P)(\mathfrak{p})}, A_\mathfrak{p}) \cong A_\mathfrak{p}^{\mathrm{rank}(P)(\mathfrak{p})}.$$

These verify the assertions of ranks. □

Proposition 3.1.7. *Let B be an A-algebra and P a projective A-module. Then $P \otimes_A B$ is a projective B-module. Moreover, if P is finitely generated, the following diagram commutes.*

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

Proof. Let Q be such that $P \oplus Q$ is a free A-modules. Then $(P \otimes_A B) \oplus (Q \otimes_A B) \cong (P \oplus Q) \otimes_A B$ is a free B-module. This verifies the first assertion. Now suppose P is finitely generated projective and $A \xrightarrow{\varphi} B$ makes B an A-algebra. Then for any $\mathfrak{p} \in \operatorname{Spec} B$, we have

$$\begin{aligned} B_\mathfrak{p}^{\mathrm{rank}(P\otimes_A B)(\mathfrak{p})} &\cong (P \otimes_A B)_\mathfrak{p} \cong P \otimes_A B_\mathfrak{p} \\ &\cong P \otimes_A A_{\varphi^{-1}(\mathfrak{p})} \otimes_{A_{\varphi^{-1}(\mathfrak{p})}} B_\mathfrak{p} \cong P_{\varphi^{-1}(\mathfrak{p})} \otimes_{A_{\varphi^{-1}(\mathfrak{p})}} B_\mathfrak{p} \\ &\cong A_{\varphi^{-1}(\mathfrak{p})}^{\mathrm{rank}(P)(\varphi^{-1}(\mathfrak{p}))} \otimes_{A_{\varphi^{-1}(\mathfrak{p})}} B_\mathfrak{p} \cong B_\mathfrak{p}^{\mathrm{rank}(P)(\varphi^{-1}(\mathfrak{p}))}, \end{aligned}$$

i.e., $\mathrm{rank}(P \otimes_A B)(\mathfrak{p}) = \mathrm{rank}(P)(\varphi^{-1}(\mathfrak{p}))$. This completes the proof. □

Definition 3.1.4. Let B be an A-algebra. B is said to be *finite projective* if B is finitely generated projective as an A-module. For such an algebra we write $[B : A]$ in stead of $\mathrm{rank}_A(B)$, which is a continuous function $\operatorname{Spec} A \to \mathbb{Z}$.

Proposition 3.1.8. *Let $f : A \to B$ be a ring homomorphism making B be a finite projective A-algebra. Then we have:*

(a) f is injective $\Leftrightarrow [B : A] \geq 1$.

(b) The following three assertions are equivalent:

(i) f is surjective;

(ii) $[B : A] \leq 1$;

(iii) the map $B \otimes_A B \to B$, $x \otimes y \mapsto xy$ is an isomorphism.

(c) f is an isomorphism $\Leftrightarrow [B : A] = 1$.

Proof. (a): " $\Rightarrow$ " Suppose there is a $\mathfrak{p} \in \operatorname{Spec} A$ with $[B : A](\mathfrak{p}) = 0$, i.e., $B_\mathfrak{p} = 0$. Since $A_\mathfrak{p} \neq 0$, the map $f_\mathfrak{p} : A_\mathfrak{p} \to B_\mathfrak{p}$ is not injective, which implies f is not injective.

" $\Leftarrow$ " Now suppose $[B : A] \geq 1$. Then $\operatorname{Ker}(f_\mathfrak{p}) \subseteq \operatorname{Ann}(B_\mathfrak{p}) = 0$ since $B_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module with rank ≥ 1. Hence $\operatorname{Ker}(f)_\mathfrak{p} \cong \operatorname{Ker}(f_\mathfrak{p}) = 0$ for all $\mathfrak{p}$. So $\operatorname{Ker}(f) = 0$ thus f is injective.

(b): We will show that $(ii) \Rightarrow (i) \Rightarrow (iii) \Rightarrow (ii)$.

$(ii) \Rightarrow (i)$ We may assume that A is local with maximal ideal $\mathfrak{m}$. By Proposition 3.1.3, $[B : A]$ is constant. If $[B : A] = 0$, $\Rightarrow B = 0 \Rightarrow f$ is surjective. If $[B : A] = 1$, then B is free of rank 1. Let b is a basis of B over A, $\forall x \in B$, there is an $a_x \in A$ such that $x = a_x \cdot b$. Then for any $\alpha \in \operatorname{End}_A(B)$, we have

$$\alpha(x) = \alpha(a_x \cdot b) = a_x a_{\alpha(b)} b = a_{\alpha(b)} \cdot x.$$

Thus $\alpha = a_{\alpha(b)} \cdot \mathrm{id}_B$. This means $\operatorname{End}_A(B)$ is a free A-algebra of rank 1 with basis id_B. Then the map $g : B \to \operatorname{End}_A(B)$ defined by $b \mapsto (m_b : x \mapsto bx)$ is A-linear and injective since $m_b(1) = b$. Next we consider the composite

$$A \xrightarrow{f} B \xrightarrow{g} \operatorname{End}_A(B)$$

with $1_A \mapsto 1_B \mapsto \mathrm{id}_B$. This implies $g \circ f$ is an isomorphism. Since g is injective, f is surjective.

$(i) \Rightarrow (iii)$ Suppose f is surjective and let I denote the kernel of f thus $B \cong A/I$. Then we have a composite with natural isomorphisms

$$B \otimes_A B \xrightarrow{\sim} B \otimes_A A/I \xrightarrow{\sim} B/IB = B/f(I)B = B \text{ with}$$

$$x \otimes y \longmapsto x \otimes \overline{a} \text{ (where } f(a) = y) \longmapsto \overline{a \cdot x} = \overline{f(a)x} = xy.$$

This means the map $B \otimes_A B \to B$, $x \otimes y \mapsto xy$ is an isomorphism.

$(iii) \Rightarrow (ii)$ Now suppose $B \otimes_A B \cong B$. By Proposition 3.1.6, $[B : A] = [B \otimes_A B : A] = [B : A]^2$. So $[B : A] \geq 1$.

(c) follows immediately from (a) and (b). □

Definition 3.1.5. An A-algebra B is called *faithfully projective* if it is finite projective with $[B : A] \geq 1$, i.e., if it is faithfully projective as an A-module.

By Proposition 3.1.4 we see that B is faithfully projective if and only if it is faithfully flat. Next we give some equivalent statements for faithfully flat algebras.

Proposition 3.1.9. *Let B be a flat A-algebra. Then the following conditions are equivalent:*

(i) $\mathfrak{a}^{ec} = \mathfrak{a}$ *for all ideals* $\mathfrak{a}$ *of* A.

(ii) $\operatorname{Spec} B \to \operatorname{Spec} A$ *is surjective.*

(iii) For every maximal ideal $\mathfrak{m}$ *of* A *we have* $\mathfrak{m}^e \neq (1)$.

(iv) If M *is any non-zero* A*-module, then* $M_B = M \otimes_A B \neq 0$.

(v) For every A*-module* M*, the map* $M \to M_B$ *by* $x \mapsto x \otimes 1$ *is injective.*

For the proof of this proposition, we refer to Atiyah and MacDonald (1994) Ch3, Ex. 16.

Proposition 3.1.10. *Let B be a faithfully flat A-algebra, and P an A-module. Then P is a finitely generated projective A-module if and only if $P \otimes_A B$ is a finitely generated projective B-module.*

Proof. By Proposition 3.1.7 the "only if" part is always true for any A-algebra B. Conversely, we assume that $P \otimes_A B$ is a finitely generated projective B-module. Then we can choose a finite set of generators of the form $p_1 \otimes 1, p_2 \otimes 1, \dots p_n \otimes 1$ with $p_i \in P$ for all i. Let $e_1, e_2, \dots, e_n$ be the standard basis of A^n and define a map

$$\varphi : A^n \longrightarrow P, \quad e_i \mapsto P_i.$$

Then $\varphi \otimes \mathrm{id}_B : A^n \otimes_A B \longrightarrow P \otimes_A B$ is surjective. Since B is faithfully projective, φ is also surjective by Proposition 3.1.4. Thus P is finitely generated. Let $Q = \mathrm{Ker}(\varphi)$. Using B faithfully projective again, the exact sequence

$$0 \longrightarrow Q \otimes_A B \longrightarrow A^n \otimes_A B \longrightarrow P \otimes_A B \longrightarrow 0$$

splits. Hence $B^n \cong A^n \otimes_A B \cong (P \otimes_A B) \oplus (Q \otimes_A B)$, which implies $Q \otimes_A B$ is finitely generated projective. Applying the same proof we give for P to $Q \otimes_A B$ we obtain that Q is finitely generated. This shows that P is finitely presented.

Now we take an arbitrary A-module M. First we claim that the natural map

$$\psi : \mathrm{Hom}_A(P, M) \otimes_A B \longrightarrow \mathrm{Hom}_B(P \otimes_A B, M \otimes_A B), \quad f \otimes 1 \mapsto f \otimes \mathrm{id}_B$$

is an isomorphism of B-modules. If $P \cong A^m$ for some $m < \infty$, this claim is true by the following commutative diagram,

$$\begin{tikzcd}
\mathrm{Hom}_A(A^m, M) \otimes_A B \arrow[r, "\psi"] & \mathrm{Hom}_B(A^m \otimes_A B, M \otimes_A B) \\
\big(\mathrm{Hom}_A(A, M)\big)^m \otimes_A B \arrow[u, "\sim"'] & \mathrm{Hom}_B(B^m, M \otimes_A B) \arrow[u, "\sim"'] \\
M^m \otimes_A B \arrow[u, "\sim"'] & \big(\mathrm{Hom}_B(B, M \otimes_A B)\big)^m \arrow[u, "\sim"'] \\
(M \otimes_A B)^m \arrow[u, "\sim"'] \arrow[r, equal] & (M \otimes_A B)^m \arrow[u, "\sim"']
\end{tikzcd}$$

by

$$
\begin{tikzcd}
(e_i \mapsto x_i) \otimes 1_B \arrow[r, mapsto] & (e_i \otimes 1_B \mapsto x_i \otimes 1_B) \\
\big((1_A \mapsto x_1), \ldots, (1_A \mapsto x_m)\big) \otimes 1_B \arrow[u, mapsto] & (e_i' \mapsto x_i \otimes 1_B) \arrow[u, mapsto] \\
(x_1, \ldots x_m) \otimes 1_B \arrow[u, mapsto] & \big((1_B \mapsto x_1 \otimes 1_B), \ldots, (1_B \mapsto x_m \otimes 1_B)\big) \arrow[u, mapsto] \\
(x_1 \otimes 1_B, \ldots, x_m \otimes 1_B) \arrow[u, mapsto] \arrow[r, equal] & (x_1 \otimes 1_B, \ldots, x_m \otimes 1_B) \arrow[u, mapsto]
\end{tikzcd}
$$

where all the isomorphisms are natural and e_i's, e_i''s are standard basis for A^m, B^m respectively. For general P, we choose an exact sequence $A^m \to A^n \to P \to 0$. Then we have a commutative diagram

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

Both rows are exact by left exactness of $\mathrm{Hom}_A(-, M)$ and flatness of B. Then by what we just proved for free modules and five lemma, ψ is an isomorphism.

Now let $M \to N \to 0$ be an exact sequence of A-modules. We have

$M \otimes_A B \to N \otimes_A B \to 0$ (B is flat).

$\Rightarrow$ $\mathrm{Hom}_B(P \otimes_A B, M \otimes_A B) \to \mathrm{Hom}_B(P \otimes_A B, N \otimes_A B) \to 0$ is exact

($P \otimes_A B$ is projective).

$\Rightarrow$ $\mathrm{Hom}_A(P, M) \otimes_A B \to \mathrm{Hom}_A(P, N) \otimes_A B \to 0$ is exact.

$\Rightarrow$ $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N) \to 0$ is exact (B is faithfully projective).

$\Rightarrow$ P is finitely generated projective over A.

This completes the proof. □

Let P be a finitely generated projective A-module and $P^\vee = \mathrm{Hom}_A(P, A)$ denote the dual module of P. Using Proposition 3.1.5, let $M = P$, we get an isomorphism

$$\phi : P^\vee \otimes_A P \to \mathrm{Hom}_A(P, P) = \mathrm{End}_A(P) \quad \text{with} \quad f \otimes q \mapsto (p \mapsto f(p) \cdot q).$$

We define the *trace* map $\mathrm{tr} = \mathrm{tr}_{P/A} : \mathrm{End}_A(P) \to A$ to be the composite

$$\mathrm{End}_A(P) = \mathrm{Hom}_A(P, P) \xrightarrow{\phi^{-1}} P^\vee \otimes_A P \longrightarrow A,$$

where the second map is given by $f \otimes p \mapsto f(p)$.

Proposition 3.1.11. *Let P be a free A-module with basis $w_1, w_2, \ldots, w_n$, and define $w_i^* \in P^\vee$ by $w_i^*(w_j) = 1$ if $i = j$ and $w_i^*(w_j) = 0$ if $i \neq j$. Let $f \in \mathrm{End}_A(P)$, $f(w_i) = \sum_{j=1}^n a_{ij} w_j$ with $a_{ij} \in A$. Then we have*

(a) $P^\vee$ is a free A-module with basis $w_1^*, w_2^*, \ldots, w_n^*$.

(b) $\phi^{-1}(f) = \sum\limits_{i,j} a_{ij} w_i^* \otimes w_j$.

(c) $\mathrm{tr}_{P/A}(f) = \sum\limits_{i=1}^n a_{ii}$.

Proof. (a): Clearly $P^\vee$ is a free A-module of rank n. It suffices to show that the w_i^*'s generate $P^\vee$. Take an arbitrary $g \in P^\vee$. For any $x \in P$, there exists $a_1, \ldots, a_n \in A$ such that $x = \sum_{i=1}^n a_i w_i$. Then

$$\begin{aligned} \sum_{i=1}^n g(w_i) w_i^*(x) &= \sum_{i=1}^n g(w_i) w_i^*(\sum_{j=1}^n a_j w_j) = \sum_{i=1}^n g(w_i) \sum_{j=1}^n a_j w_i^*(w_j) \\ &= \sum_{i=1}^n g(w_i) a_i = g(\sum_{i=1}^n a_i w_i) = g(x) \end{aligned}$$

This implies $g = \sum\limits_{i=1}^n g(w_i) w_i^*$.

(b): Since ϕ is an isomorphism, it is enough to show that $\phi(\sum_{i,j} a_{ij} w_i^* \otimes w_j) = f$. We shall check this on the generators. For any $1 \leq k \leq n$, we have

$$\phi(\sum_{i,j} a_{ij} w_i^* \otimes w_j)(w_k) = \sum_{i,j} a_{ij} w_i^*(w_k) \cdot w_j) = \sum_{j=1}^n a_{kj} w_j = f(w_k).$$

(c): The image of f under the trace map is:

$$\begin{array}{rccccc} \mathrm{tr}_{P/A}(f): & \mathrm{End}_A(P) & \xrightarrow{\phi} & P^\vee \otimes_A P & \longrightarrow & A \\ & f & \longmapsto & \sum\limits_{i,j} a_{ij} w_i^* \otimes w_j & \longmapsto & \sum\limits_{i,j} a_{ij} w_i^*(w_j) = \sum\limits_{i=1}^n a_{ii}. \end{array}$$

This completes the proof. $\square$

Remark 3.1.3. In the special case $P = A$, for any $f \in \mathrm{End}_A(A)$, we have $\mathrm{tr}_{A/A}(f) = f(1)$ by part (c) of the above proposition.

We have the following properties for the trace map.

Proposition 3.1.12. *Let B be an A-algebra and P a finitely generated projective A-module. Then the following diagram of natural maps*

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

is commutative.

Proof. Let $p_1, p_2, \ldots, p_n$ be the generators of P as an A-module, then $p_1 \otimes 1, p_2 \otimes 1, \ldots, p_n \otimes 1$ generate $P \otimes_A B$ as a B-module. For any $f \in P^\vee$, f induces a B-linear map $\widetilde{f} : P \otimes_A B \to B$ with $\widetilde{f}(p\otimes b) = f(p)\cdot b$. Recall that the map $\phi : P^\vee \otimes_A P \to \mathrm{End}_A(P)$ is defined by $f \otimes p' \mapsto (p \mapsto f(p)\cdot p')$. Then for any $x \in P$ and $b \in B$, we have

$$\begin{aligned} \phi(\widetilde{f} \otimes (p \otimes 1))(x \otimes b) &= \widetilde{f}(x \otimes b) \cdot (p \otimes 1) = f(x)b \cdot (p \otimes 1) \\ &= f(x) \cdot p \otimes b = \phi(f \otimes p)(x) \otimes b \\ &= \phi(f \otimes p)(x) \otimes \mathrm{id}_B(b) = \Big(\phi(f \otimes p) \otimes \mathrm{id}_B\Big)(x \otimes b). \end{aligned}$$

Hence the following diagram

$$\begin{tikzcd} \mathrm{End}_A(P) \arrow[r, "\phi^{-1}"] \arrow[d, "\otimes \mathrm{id}_B"] \arrow[rr, bend left, "\mathrm{tr}_{P/A}"] & P^\vee \otimes_A P \arrow[r] & A \arrow[d] \\ \mathrm{End}_B(P \otimes_A B) \arrow[r, "\phi^{-1}"] \arrow[rr, bend right, "\mathrm{tr}_{P\otimes_A B/B}"'] & (P \otimes_A B)^\vee \otimes_B (P \otimes_A B) \arrow[r] & B \end{tikzcd}$$

is commutative by

$$
\begin{tikzcd}
g \arrow[r, mapsto] \arrow[d, mapsto] \arrow[rr, mapsto, bend left] & \sum\limits_{i\in I} f_i \otimes p_i \arrow[r, mapsto] & \sum\limits_{i\in I} f_i(p_i) \arrow[d, mapsto] \\
 & & \sum\limits_{i\in I} f_i(p_i)\cdot 1 \arrow[d, equal] \\
g \otimes \mathrm{id}_B \arrow[r, mapsto] \arrow[rr, mapsto, bend right] & \sum\limits_{i\in I} \widetilde{f}_i \otimes (p_i \otimes 1) \arrow[r, mapsto] & \sum\limits_{i\in I} \widetilde{f}_i(p_i \otimes 1),
\end{tikzcd}
$$

where I is a finite index set. This completes the proof. $\square$

Proposition 3.1.13. *Let $0 \to P_0 \to P_1 \to P_2 \to 0$ be an exact sequence of A-modules in which P_1 and P_2 are finitely generated projective, and $g : P_1 \to P_1$ an A-linear map with $g[P_0] \subset P_0$. Denote by h the induced map $P_2 \to P_2$. Then P_0 is finitely generated projective and $\mathrm{tr}_{P_1/A}(g) = \mathrm{tr}_{P_0/A}(g|_{P_0}) + \mathrm{tr}_{P_2/A}(h)$.*

Proof. Let Q be such that $P_1 \oplus Q$ is a free A-module of finite rank. The assumption that P_2 is projective implies $P_1 \cong P_0 \oplus P_2$. Then $P_1 \oplus Q \cong P_0 \oplus P_2 \oplus Q \cong P_0 \oplus Q_1$ proves the first claim. Since $P_1 \cong P_0 \oplus P_2$, we have the following diagram:

$$
\begin{tikzcd}[column sep=small]
\mathrm{End}_A(P_1) \arrow[r, "\sim"] \arrow[d, "\phi^{-1}"', "\sim"] & \mathrm{End}_A(P_0) \arrow[d, "\sim"', "\phi_1^{-1}"] \oplus & \mathrm{Hom}_A(P_0, P_2) \arrow[d, "\sim"', "\phi_2^{-1}"] \oplus & \mathrm{Hom}_A(P_2, P_0) \arrow[d, "\sim"', "\phi_3^{-1}"] \oplus & \mathrm{End}_A(P_2) \arrow[d, "\sim"', "\phi_4^{-1}"] \\
P_1^\vee \otimes_A P_1 \arrow[r, "\sim"] \arrow[d] & (P_0^\vee \otimes_A P_0) \oplus & (P_0^\vee \otimes_A P_2) \arrow[d] \oplus & (P_2^\vee \otimes_A P_0) \oplus & (P_2^\vee \otimes_A P_2) \\
A \arrow[rr, equal] & & A, & &
\end{tikzcd}
$$

where $\phi_1, \phi_2, \phi_3, \phi_4$ are isomorphisms given in Proposition 3.1.5 and the second arrow in the right column is the sum of the two maps $P_0^\vee \otimes_A P_0 \to A$ and $P_2^\vee \otimes_A P_2 \to A$. Then the composite of the maps in the second column is just $\mathrm{tr}_{P_0/A} + \mathrm{tr}_{P_2/A}$. The above diagram is commutative by

$$
\begin{tikzcd}
g \arrow[r, mapsto] \arrow[d, mapsto] & \big(\pi_0 g \varphi_0, \pi_2 g \varphi_0, \pi_0 g \varphi_2, \pi_2 g \varphi_2\big) \arrow[d, mapsto] \\
f \otimes m \arrow[r, mapsto] \arrow[d, mapsto] & \Big(f\varphi_0 \otimes \pi_0(m), f\varphi_0 \otimes \pi_2(m), f\varphi_2 \otimes \pi_0(m), f\varphi_2 \otimes \pi_2(m)\Big) \arrow[d, mapsto] \\
f(m) \arrow[r, equal] & f\big(\varphi_0\pi_0(m) + \varphi_2\pi_2(m)\big),
\end{tikzcd}
$$

where φ_j is the natural inclusion $P_j \to P_1$ and π_j is the natural projection $P_1 \to P_j$ for $j = 0, 2$. Actually, the image of $g \in \mathrm{End}_A(P_1)$ under ϕ^{-1} is of the form $\sum_{i \in I} f_i \otimes m_i$ with I finite. Since all the arrows in the diagram are A-linear, we may assume that it is of the from $f \otimes m$. Then we have $\mathrm{tr}_{P_1/A}(g) = \mathrm{tr}_{P_0/A}(\pi_0 g \varphi_0) + \mathrm{tr}_{P_2/A}(\pi_2 g \varphi_2)$.

Indeed, $g|_{P_0} = \pi_0 g \varphi_0$ since $g[P_0] \subset P_0$. Moreover, the induced map $h : P_2 \to P_2$ is just $\pi_2 g \varphi_2$. Thus $\mathrm{tr}_{P_1/A}(g) = \mathrm{tr}_{P_0/A}(g|_{P_0}) + \mathrm{tr}_{P_2/A}(h)$. $\square$

Proposition 3.1.14. *Let P and Q be two finitely generated projective A-modules and $f : P \to Q$, $g : Q \to P$ two A-linear maps. Then*

$$\mathrm{tr}_{P/A}(g \circ f) = \mathrm{tr}_{Q/A}(f \circ g).$$

Proof. By Proposition 3.1.5 we have

$$P^\vee \otimes_A Q \xrightarrow[\phi]{\sim} \mathrm{Hom}_A(P, Q) \qquad \text{and} \qquad Q^\vee \otimes_A P \xrightarrow[\phi]{\sim} \mathrm{Hom}_A(Q, P).$$

Let $\phi^{-1}(f) = \sum_{j \in J} f_j \otimes q_j$ and $\phi^{-1}(g) = \sum_{i \in I} g_i \otimes p_i$, where I, J are finite set and $f_j \in P^\vee$, $g_i \in Q^\vee$, $q_j \in Q$, $p_i \in P$. Then for any $p \in P$, we have

$$\begin{aligned} \phi\Big(\sum_{i,j} f_j \otimes g_i(q_j) p_i\Big)(p) &= \sum_{i,j} f_j(p) \cdot g_i(q_j) p_i = \sum_j f_j(p) \sum_i g_i(q_j) p_i \\ &= \sum_j f_j(p) g(q_j) = g\big(\sum_j f_j(p) q_j\big) = g \circ f(p), \end{aligned}$$

i.e., $\phi^{-1}(g \circ f) = \sum_{i,j} f_j \otimes g_i(q_j) p_i$. Similarly we can show that $\phi^{-1}(f \circ g) = \sum_{i,j} g_i \otimes f_j(p_i) q_j$. So by the definition of the trace map, we have

$$\mathrm{tr}_{Q/A}(f \circ g) = \sum_{i,j} g_i\big(f_j(p_i) q_j\big) = \sum_{i,j} g_i(q_j) f_j(p_i) = \sum_{i,j} f_j\big(g_i(q_j) p_i\big) = \mathrm{tr}_{Q/A}(g \circ f).$$

This verifies the statement. $\square$

Proposition 3.1.15. *Let $B_1, B_2, \ldots, B_n$ be algebras over A. Then $\prod_{i=1}^{n} B_i$ is finite projective over A if and only if each B_i is finite projective over A.*

Proof. This follows from Lemma 3.1.1 immediately. □

Proposition 3.1.16. *Let B be a finite projective A-algebra and P a finitely generated projective B-module. Then P is a finitely generated projective A-module.*

Proof. Clearly, P is finitely generated as an A-module. Let M be an A-module such that $B \oplus M \cong A^n$ and Q be a B-module such that $P \oplus Q \cong B^m$ for some $m, n < \infty$. Then $A^{mn} \cong \bigoplus_{i=1}^{n} (B \oplus M)^m \cong P \oplus Q'$ verifies the assertion. □

3.2 Separable algebras

Let B be a finite projective A-algebra. For any $b \in B$, let $m_b : B \to B$ be map defined by the multiplication by b, i.e., $m_b(x) = bx$ for any $x \in B$. Then we define the *trace* map

$$\mathrm{Tr}_{B/A} : B \to A, \quad \text{by} \quad b \mapsto \mathrm{tr}(m_b).$$

This map is A-linear and induces another A-linear map

$$\psi : B \to \mathrm{Hom}_A(B, A) \quad \text{by} \quad \psi(b)(b') = \mathrm{Tr}_{B/A}(bb') \text{ for } b, b' \in B.$$

Proposition 3.2.1. *Let B be a finite projective A-algebra and C a finite projective B-algebra. Then C is a finite projective A-algebra and* $\mathrm{Tr}_{C/A} = \mathrm{Tr}_{B/A} \circ \mathrm{Tr}_{C/B}$.

Proof. The first claim follows immediately from Proposition 3.1.16. For the second assertion, first, we claim that the natural homomorphism

$$\Phi : \mathrm{Hom}_A(C, A) \otimes_A B \longrightarrow \mathrm{Hom}_A(C, B), \quad f \otimes b \longmapsto (f_b : c \mapsto f(c) \cdot b)$$

is an isomorphism. This is true if $C = B^n$ for some $n < \infty$, since both sides may be identified with $\big(\mathrm{End}_A(B)\big)^n$ and the map Φ coincides with the identity map on $\big(\mathrm{End}_A(B)\big)^n$. In the general case we choose an exact sequence $B^m \to B^n \to C \to 0$. Then we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_A(C,B) \arrow[r] & \mathrm{Hom}_A(B^n,B) \arrow[r] & \mathrm{Hom}_A(B^m,B) \\
0 \arrow[r] & \mathrm{Hom}_A(C,A)\otimes_A B \arrow[r] \arrow[u, "\Phi"'] & \mathrm{Hom}_A(B^n,A)\otimes_A B \arrow[r] \arrow[u, "\cong"'] & \mathrm{Hom}_A(B^m,A)\otimes_A B \arrow[u, "\cong"']
\end{tikzcd}$$

with both rows exact. So Φ is an isomorphism.

Consider the following diagram

$$\begin{tikzcd}
C \arrow[rrr, equal] \arrow[d] & & & C \arrow[d] \\
\mathrm{End}_B(C) \arrow[rrr] \arrow[d, "\phi^{-1}"] & & & \mathrm{End}_A(C) \arrow[d, "\phi^{-1}"] \\
\mathrm{Hom}_B(C,B)\otimes_B C \arrow[r] \arrow[d] & \mathrm{Hom}_A(C,B)\otimes_B C \arrow[r] & \mathrm{Hom}_A(C,A)\otimes_A B\otimes_B C \arrow[r] & \mathrm{Hom}_A(C,A)\otimes_A C \arrow[d] \\
B \arrow[r] & \mathrm{End}_A(B) \arrow[rr, "\mathrm{tr}_{B/A}"] & & A,
\end{tikzcd}$$

whose map is given by

$$\begin{tikzcd}
y \arrow[rrr, equal] \arrow[d, mapsto] & & & y \arrow[d, mapsto] \\
m_y \arrow[rrr, mapsto] \arrow[d, mapsto] & & & m_y \arrow[d, mapsto] \\
f\otimes c \arrow[r, mapsto] \arrow[dd, mapsto] & f\otimes c \arrow[r, mapsto] & \Big(\sum\limits_{j\in J} g_j\otimes b_j\Big)\otimes c \arrow[r, mapsto] & \sum\limits_{j\in J} g_j\otimes b_j c \arrow[d, mapsto] \\
& & & \sum\limits_{j\in J} g_j(b_j c) \arrow[d, equal, "?"] \\
f(c) \arrow[r, mapsto] & m_{f(c)} \arrow[rr, mapsto] & & \mathrm{tr}_{B/A}(m_{f(c)})
\end{tikzcd}$$

with I, J finite index sets and $\Phi\Big(\sum\limits_{j\in J} g_j\otimes b_j\Big) = f$. The first arrow in the right column is verified by

$$\begin{aligned}
\phi\Big(\sum_{j\in J} g_j\otimes b_j c\Big)(d) &= \sum_{j\in J} g_j(d)(b_j c) \quad (\forall d\in C) \\
&= \Big(\sum_{j\in J} g_j(d) b_j\Big)c = \Phi\Big(\sum_{j\in J} g_j\otimes b_j\Big)(d)c \\
&= f(d)c = \phi(f\otimes c)(d) = m_y(d).
\end{aligned}$$

The proof of $\mathrm{Tr}_{C/A} = \mathrm{Tr}_{B/A} \circ \mathrm{Tr}_{C/B}$ is equivalent to showing that the above diagram is commutative. So it suffices to show that $\mathrm{tr}_{B/A}(m_{f(c)}) = \sum\limits_{j\in J} g_j(b_j c)$. Let μ_j be the map $A \to B$, $a \mapsto a \cdot b_j$ and μ_c be $B \to C$, $b \mapsto b \cdot c$. Notice that $\Phi\Big(\sum\limits_{j\in J} g_j \otimes b_j\Big) = f$, then for any $z \in B$, since f is B-linear, we have

$$\begin{aligned} m_{f(c)}(z) &= f(c)z = f(z\cdot c) = \Phi\Big(\sum_{j\in J} g_j \otimes b_j\Big)(z\cdot c) \\ &= \sum_{j\in J} b_j g_j(zc) = \sum_{j\in J} (\mu_j \circ g_j \circ \mu_c)(c), \end{aligned}$$

i.e., $m_{f(c)} = \sum\limits_{j\in J} \mu_j \circ g_j \circ \mu_c$. Then by the linearity and Proposition 3.1.14, we conclude that

$$\begin{aligned} \mathrm{tr}_{B/A}(m_{f(c)}) &= \mathrm{tr}_{B/A}\Big(\sum_{j\in J} \mu_j \circ g_j \circ \mu_c\Big) = \sum_{j\in J} \mathrm{tr}_{B/A}\big(\mu_j \circ (g_j \circ \mu_c)\big) \\ &= \sum_{j\in J} \mathrm{tr}_{A/A}\big((g_j \circ \mu_c) \circ \mu_j\big) = \sum_{j\in J} (g_j \circ \mu_c \circ \mu_j)(1) \\ &= \sum_{j\in J} g_j(cb_j) = \sum_{j\in J} g_j(b_j c). \end{aligned}$$

So $\mathrm{Tr}_{C/A} = \mathrm{Tr}_{B/A} \circ \mathrm{Tr}_{C/B}$. This completes the proof. $\square$

Definition 3.2.1. A finite projective A-algebra B is said to be *separable* if the map $\psi : B \to \mathrm{Hom}_A(B, A)$ defined at the beginning of this section is an isomorphism. In what follows, we will call projective separable algebras as separable algebras for convenience.

Next we will give an example of separable algebra.

Example 3.2.1. Let $B = A^n$ with $n < \infty$, where multiplication is defined componentwise. B is an A-algebra via the homomorphism given by

$$A \longrightarrow B, \quad a \mapsto (a, a, \ldots, a).$$

Then B is a finite projective A-algebra. Let $e_1, \ldots, e_n$ be the standard A-basis for B. For any $x = (x_1, x_2, \ldots, x_n) \in B$, the map $m_x : B \to B$ defined by $y \mapsto xy$ sends e_i to $x_i \cdot e_i$. Hence $\mathrm{Tr}_{B/A}(x) = \mathrm{tr}(m_x) = \sum\limits_{i=1}^{n} x_i$ by Proposition 3.1.11.

Recall that the map $\psi : B \to \mathrm{Hom}_A(B, A)$ is given by $x \mapsto (e_i \mapsto \mathrm{Tr}_{B/A}(xe_i) = x_i)$. Define $\alpha : \mathrm{Hom}_A(B, A) \to B$ by $f \mapsto (f(e_1), \ldots, f(e_n))$. Clearly α is A-linear with

$$(\alpha \circ \psi)(x) = \alpha(e_i \mapsto x_i) = (x_1, \ldots, x_n) = x \text{ and}$$

$$(\psi \circ \alpha)(f) = \psi(f(e_1), \ldots, f(e_n)) = (e_i \mapsto \mathrm{Tr}_{B/A}((f(e_1), \ldots, f(e_n))e_i) = f(e_i)) = f.$$

Hence ψ is an isomorphism and $B \cong A^n$ is separable.

Proposition 3.2.2. *Let $B_1, B_2, \ldots, B_n$ be algebras over A. Then $\prod_{i=1}^{n} B_i$ is separable over A if and only if each B_i is separable over A.*

Proof. Let $B = \prod_{i=1}^n B_i$. By Proposition 3.1.15, B is finite projective if and only if B_i is finite projective. It suffices to show that $\psi : B \to \mathrm{Hom}_A(B, A)$ is an isomorphism if and only if $\psi_i : B_i \to \mathrm{Hom}_A(B_i, A)$ is an isomorphism for each i. Let φ_i denote the natural map $B_i \to B$ and π_i the projection $B \to B_i$. As in the proof of Proposition 3.1.13 we can show a similar assertion that for any $b = (b_1, b_2, \ldots, b_n) \in B$

$$\mathrm{Tr}_{B/A}(b) = \mathrm{tr}_{B/A}(m_b) = \sum_{i=1}^{n} \mathrm{tr}_{B_i/A}(\pi_i m_b \varphi_i) = \sum_{i=1}^{n} \mathrm{tr}_{B_i/A}(m_{b_i}) = \mathrm{Tr}_{B_i/A}(b_i).$$

Then the following diagram

$$\begin{tikzcd}
B \arrow[rr, "\pi_i"] \arrow[d, "\psi"'] & & B_i \arrow[d, "\psi_i"] \\
\mathrm{Hom}_A(B, A) \arrow[r, "\sim"'] & \prod_{i=1}^{n} \mathrm{Hom}_A(B_i, A) \arrow[r, "\pi_i"] & \mathrm{Hom}_A(B_i, A)
\end{tikzcd}$$

is commutative, where the arrows are given by

$$\begin{tikzcd}
b = (b_i)_{i=1}^n \arrow[rr, mapsto] \arrow[d, mapsto] & & b_i \arrow[d, mapsto] \\
\big(x = (x_i)_{i=1}^n \mapsto \mathrm{Tr}_{B/A}(bx)\big) \arrow[r, mapsto] & \Big(x_i \mapsto \mathrm{Tr}_{B/A}([b_i x_i])\Big)_{i=1}^{n} \arrow[r, mapsto] & (x_i \mapsto \mathrm{Tr}_{B_i/A}(b_i x_i)),
\end{tikzcd}$$

where $[x_i]$ denote the element $(0, \ldots, x_i, \ldots, 0)$ in B having x_i in the i-th spot and zeros elsewhere. Hence $\mathrm{Tr}_{B/A}([b_i x_i]) = \mathrm{Tr}_{B_i/A}(b_i x_i)$. Then ψ is an isomorphism if and only if ψ_i is an isomorphism for each i, which completes the proof. ∎

Proposition 3.2.3. *Let B be a separable A-algebra and C a separable B-algebra. Then C is a separable A-algebra.*

Proof. First, we claim that $\mathrm{Hom}_B\big(C, \mathrm{Hom}_A(B,A)\big) \cong \mathrm{Hom}_A(C \otimes_B B, A)$. On the left hand side, we consider $\mathrm{Hom}_A(B,A)$ as a B-module by $(b' \cdot h)(b) = h(b'b)$ with $h \in \mathrm{Hom}_A(B,A)$ and $b, b' \in B$. Then for any $f \in \mathrm{Hom}_A(C \otimes_B B, A)$, define $\widetilde{f} : C \to \mathrm{Hom}_A(B,A)$ by $c \mapsto \big(f_c : b \mapsto f(c \otimes b)\big)$. It is easy to check that $\widetilde{f}$ is B-linear. Moreover, for any $g \in \mathrm{Hom}_B\big(C, \mathrm{Hom}_A(B,A)\big)$, there is an A-bilinear map $C \times B \to A$ associates to g by sending (c,b) to (g(c))(b). This induces an A-linear map $\overline{g} : C \otimes_B B \to A$ sending $c \otimes b$ to (g(c))(b). Consider the map $\mathrm{Hom}_B\big(C, \mathrm{Hom}_A(B,A)\big) \to \mathrm{Hom}_A(C \otimes_B B, A)$ by $g \mapsto \overline{g}$ and the map $\mathrm{Hom}_A(C \otimes_B B, A) \to \mathrm{Hom}_B\big(C, \mathrm{Hom}_A(B,A)\big)$ by $f \mapsto \widetilde{f}$. Then these two maps are inverse to each other, hence are isomorphisms.

We have the following commutative diagram

$$\begin{tikzcd}
C \arrow[r, "\sim", "\psi_B"'] \arrow[d, "\psi_A"'] & \mathrm{Hom}_B(C,B) \arrow[r, "\sim"] & \mathrm{Hom}_B\big(C, \mathrm{Hom}_A(B,A)\big) \arrow[d, "\sim"] \\
\mathrm{Hom}_A(C,A) & & \mathrm{Hom}_A(C \otimes_B B, A) \arrow[ll, "\sim"']
\end{tikzcd}$$

by

$$\begin{tikzcd}
c \arrow[r, mapsto] \arrow[d, mapsto] & (x \mapsto \mathrm{Tr}_{C/B}(cx)) \arrow[r, mapsto] & \Big(x \mapsto \big(b \mapsto \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(cx))b\big)\Big) \arrow[d, mapsto] \\
(x \mapsto \mathrm{Tr}_{C/A}(cx)) \arrow[r, equal] & \Big(x \mapsto \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(cx))\Big) & \Big(x \otimes b \mapsto \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(cx))b\Big), \arrow[l, mapsto]
\end{tikzcd}$$

where the " = " follows from Proposition 3.2.1. So $\psi_A : C \to \mathrm{Hom}_A(C,A)$ is an isomorphism thus C is a separable A-algebra. ☐

Proposition 3.2.4. *Let C be any A-algebra. If B is a separable A-algebra then $B \otimes_A C$ is a separable C-algebra. The converse is also true if C is faithfully flat.*

Proof. By Proposition 3.1.7, $B \otimes_A C$ is finite projective over C. It suffices to show $B \otimes_A C \cong \mathrm{Hom}_C(B \otimes_A C, C)$. First we claim that the natural map $\mathrm{Hom}_A(B,A) \otimes_A C \longrightarrow \mathrm{Hom}_C(B \otimes_A C, C)$, $f \otimes c \mapsto \Big(b' \otimes c' \mapsto f(b')cc'\Big)$ is an isomorphism of C-modules. This is clear if $B \cong A^n$ for some $n < \infty$ since both sides are isomorphic to C^n and the the natural map $\mathrm{Hom}_A(B,A) \otimes_A C \longrightarrow$

$\mathrm{Hom}_C(B \otimes_A C, C)$ coincides with the identity map on C^n. In general we localize at any $\mathfrak{p} \in \operatorname{Spec} C$ then the following diagram

$$\begin{tikzcd}
\Big(\mathrm{Hom}_C(B \otimes_A C, C)\Big)_{\mathfrak{p}} \arrow[r, "\sim"] & \mathrm{Hom}_{C_{\mathfrak{p}}}((B \otimes_A C)_{\mathfrak{p}}, C_{\mathfrak{p}}) \arrow[r, "\sim"] & \mathrm{Hom}_{C_{\mathfrak{p}}}(C_{\mathfrak{p}}^m, C_{\mathfrak{p}}) \arrow[r, "\sim"] & C_{\mathfrak{p}}^m \arrow[d, equal] \\
\mathrm{Hom}_A(B, A) \otimes_A C_{\mathfrak{p}} \arrow[u] \arrow[r, "\sim"] & \mathrm{Hom}_A(B, A) \otimes_A A_{\mathfrak{p}^c} \otimes_{A_{\mathfrak{p}^c}} C_{\mathfrak{p}} \arrow[r, "\sim"] & A_{\mathfrak{p}^c}^m \otimes_{A_{\mathfrak{p}^c}} C_{\mathfrak{p}} \arrow[r, "\sim"] & C_{\mathfrak{p}}^m
\end{tikzcd}$$

commutes, where $\mathfrak{p}^c$ is the contraction of $\mathfrak{p}$ in A. This proves the claim.

Since B is separable over A, $B \cong \mathrm{Hom}_A(B, A)$ under ψ. Then $B \otimes_A C \cong \mathrm{Hom}_A(B, A) \otimes_A C$ under $\psi \otimes \mathrm{id}_C$. The following diagram

$$\begin{tikzcd}
B \otimes_A C \arrow[r, "\psi"'] \arrow[d, equal] & \mathrm{Hom}_C(B \otimes_A C, C) \\
B \otimes_A C \arrow[r, "\psi \otimes \mathrm{id}_C", "\sim"'] & \mathrm{Hom}_A(B, A) \otimes_A C \arrow[u, "\sim"]
\end{tikzcd}$$

is commutative, where the arrows are given by

$$\begin{tikzcd}
b \otimes c \arrow[r, mapsto] \arrow[dd, equal] & \Big(b' \otimes c' \mapsto \mathrm{Tr}_{B \otimes_A C/C}(bb' \otimes cc') = \mathrm{Tr}_{B \otimes_A C/C}(bb' \otimes 1)cc'\Big) \\
& \Big(b' \otimes c' \mapsto \mathrm{Tr}_{B/A}(bb')cc'\Big) \arrow[u, equal, "\text{Prop 3.1.12}"'] \\
b \otimes c \arrow[r, mapsto] & \big(b' \mapsto \mathrm{Tr}_{B/A}(bb')\big) \otimes c. \arrow[u, mapsto]
\end{tikzcd}$$

This proves the first assertion.

Now suppose C is a faithfully flat A-algebra and $B \otimes_A C$ is projective separable over C. From Proposition 3.1.10, we see that B is finite projective over A. Moreover, the following diagram

$$\begin{tikzcd}
B \otimes_A C \arrow[r, "\psi", "\sim"'] \arrow[d, "\psi \otimes \mathrm{id}_C"] & \mathrm{Hom}_C(B \otimes_A C, C) \arrow[d, "\sim"] \\
\mathrm{Hom}_A(B, A) \otimes_A C \arrow[r, "\sim"] & \mathrm{Hom}_A(B \otimes_A C, A \otimes_A C)
\end{tikzcd}$$

commutes, where the isomorphism in the bottom row is the same as in the proof of Proposition 3.1.10 since C is faithfully flat and B is finite projective. So $\psi \otimes \mathrm{id}_C : B \otimes_A C \longrightarrow \mathrm{Hom}_A(B, A) \otimes_A C$ is an isomorphism. By the faithfully flatness of C, $\psi : B \to \mathrm{Hom}_A(B, A)$ is an isomorphism hence B is separable over A. This completes the proof. $\square$

Lemma 3.2.1. *Let B be a separable A-algebra and $f : B \to A$ an A-algebra homomorphism. Then there is an A-algebra C and an A-algebra isomorphism $g : B \xrightarrow{\sim} A \times C$ such that $f = p \circ g$, where p is the projection $A \times C \to A$.*

Proof. Clearly, $f \in \mathrm{Hom}_A(B, A)$. Since B is separable, $\psi : B \to \mathrm{Hom}_A(B, A)$ is an isomorphism. Let $e \in B$ be such that $\psi(e) = f$, i.e., $\mathrm{Tr}_{B/A}(ex) = f(x)$ for all $x \in B$. Since f is an A-algebra homomorphism, $\mathrm{Tr}_{B/A}(e) = f(1) = 1$. Furthermore, for all $x, y \in B$,

$$\mathrm{Tr}_{B/A}(exy) = f(xy) = f(x)f(y) = f(x)\,\mathrm{Tr}_{B/A}(ey) = \mathrm{Tr}_{B/A}(f(x)ey),$$

i.e., $\psi(ex) = \psi(f(x)e)$ for all $x \in B$. Since ψ is an isomorphism thus injective, we have $ex = f(x)e$. This implies $e\,\mathrm{Ker}(f) = 0$. Then the diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(f) \arrow[r] \arrow[d, "0"] & B \arrow[r, "f"] \arrow[d, "m_e"] & A \arrow[r] \arrow[d, "m_{f(e)}"] & 0 \\
0 \arrow[r] & \mathrm{Ker}(f) \arrow[r] & B \arrow[r, "f"] & A \arrow[r] & 0
\end{tikzcd}$$

commutes with both rows exact, where the first vertical arrow is just $m_e\big|_{\mathrm{Ker}(f)} = 0$ since $e\,\mathrm{Ker}(f) = 0$. Then

$$1 = \mathrm{Tr}_{B/A}(e) = \mathrm{tr}_{\mathrm{Ker}(f)/A}(0) + \mathrm{tr}_{A/A}(f(e)) = 0 + f(e) = f(e).$$

Note that we have $ex = f(x)e$ for all $x \in B$. Letting $x = 1$ we get $e^2 = f(e)e = e$, i.e., e is an idempotent of B. $1 - e \in \mathrm{Ker}(f)$ since $f(1 - e) = f(1) - f(e) = 0$. Then the map $A \to \mathrm{Ker}(f)$, $a \mapsto a(1 - e)$ makes $\mathrm{Ker}(f)$ be an A-algebra. Acturally $1 - e$ is the identity of $\mathrm{Ker}(f)$ since $(1 - e)y = y - ey = y - f(y)e = y - 0 = y$ for all $y \in \mathrm{Ker}(f)$. Then the projectivity of A implies $B \cong A \times \mathrm{Ker}(f)$, where the isomorphism $g : B \to A \times \mathrm{Ker}(f)$ is given by $x \mapsto (f(x), x - ef(x))$. Using the identity $ex = f(x)e$ and the fact that f is an A-algebra homomorphism, we have

$$\begin{aligned}
g(xy) &= \Big(f(xy), xy - ef(xy)\Big) \\
&= \Big(f(xy), xy - ef(y)f(x) - ef(x)f(y) + e^2 f(x)f(y)\Big) \\
&= \Big(f(x)f(y), xy - eyf(x) - exf(y) + e^2 f(x)f(y)\Big)
\end{aligned}$$

$$
\begin{aligned}
&= \Big(f(x)f(y), (x - ef(x))y - (x - ef(x))ef(y)\Big) \\
&= \Big(f(x)f(y), (x - ef(x))(y - ef(y))\Big) \\
&= \big(f(x), x - ef(x)\big)\big(f(y), y - ef(y)\big) \\
&= g(x)g(y),
\end{aligned}
$$

for all $x, y \in B$. So g is also an isomorphism of A-algebras. Furthermore, for any $x \in B$, $p \circ g(x) = p\big(f(x), x - ef(x)\big) = f(x)$, i.e., $p \circ g = f$. $\square$

Remark 3.2.1. If B is a separable A-algebra, from Proposition 3.2.4 we see that $B \otimes_A B$ is a separable B-algebra via the second factor. Moreover, the map $f : B \otimes_A B \to B$, $b \otimes b' \mapsto bb'$ is a B-algebra homomorphism. If we apply Lemma 3.2.1 to f, there is a B-algebra C and a B-algebra isomorphism $g : B \otimes_A B \xrightarrow{\sim} B \times C$ making the following diagram

$$
\begin{tikzcd}
B \otimes_A B \arrow[r, "g"] \arrow[dr, "f"'] & B \times C \arrow[d, "p"] \\
& B
\end{tikzcd}
$$

commute, where p is the first projection.

3.3 Finite étale coverings

Definition 3.3.1. Let $f : Y \to X$ be a morphism of schemes. We call f *affine* if there is an open affine cover $\{U_i\}$ of X such that $f^{-1}(U_i)$ is affine for each i.

Proposition 3.3.1. *A morphism $f : Y \to X$ of schemes is affine if and only if for every open affine $U \subseteq X$, $f^{-1}(U)$ is affine.*

Proof. The "if" part is clear by the definition. To prove the "only if" part, let $U = \operatorname{Spec} A$ be an open affine subset of X. As in the proof of Hartshorne (1977), Ch II, Proposiiton 3.2, there is an open affine cover of U, $U = \bigcup_{i \in I} U_i$ with $U_i = \operatorname{Spec} A_{f_i}$ for some $f_i \in A$ such that $f^{-1}(U_i)$ is affine for each i. This implies the morphism $f\big|_{f^{-1}(U)} : f^{-1}(U) \to U$ is affine.

So we have reduced to proving the following statement: Let $X = \operatorname{Spec} A$ be an affine scheme and a morphism $f : Y \to X$ is affine. Then Y is affine. By the above argument, we can cover X by open affine subsets $\{U_i = \mathrm{D}(f_i) = \operatorname{Spec} A_{f_i}\}_{i \in I}$ with $f_i \in A$ such that $f^{-1}(U_i)$ is affine. Furthermore, we can assume that I is finite, say $X = \bigcup_{i=1}^n \mathrm{D}(f_i)$. Taking global sections, f induces a morphism $\varphi : A \to \Gamma(Y, \mathcal{O}_Y) \triangleq B$. Let $g_i = \varphi(f_i)$ then $g_1, g_2, \ldots, g_n$ generate B since $A = \sum_{i=1}^n Af_i$. Write $f^{-1}(\mathrm{D}(f_i)) = \operatorname{Spec} B_i$. Recall that $Y_g = \{y \in Y : g_y \notin \mathfrak{m}_y \subset \mathcal{O}_y\}$ for any $g \in \Gamma(Y, \mathcal{O}_Y)$ (see Hartshorne (1977), Ch II, Ex. 2.16). Then $Y_{g_i} \cap f^{-1}(\mathrm{D}(f_j)) = \mathrm{D}\left(g_i\big|_{f^{-1}(\mathrm{D}(f_j))}\right)$. Let φ_i be the ring homomorphism $A_{f_i} \to B_i$ induced by $f\big|_{f^{-1}(\mathrm{D}(f_i))}$. Then the following diagram

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow & & \downarrow \\ A_{f_j} & \xrightarrow{\varphi_i} & B_j \end{array}$$

commutes, where the second vertical arrow is just the restriction of the global sections. Hence $\varphi_j(\frac{f_i}{1}) = \varphi(f_i)\big|_{f^{-1}(\mathrm{D}(f_j))}$. Then we have

$$\begin{aligned} Y_{g_i} \cap f^{-1}(\mathrm{D}(f_j)) &= \mathrm{D}\left(g_i\big|_{f^{-1}(\mathrm{D}(f_j))}\right) \\ &= \{\mathfrak{p} \in \operatorname{Spec} B_j : g_i\big|_{f^{-1}(\mathrm{D}(f_j))} \notin \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} B_j : \varphi(f_i)\big|_{f^{-1}(\mathrm{D}(f_j))} \notin \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} B_j : \varphi_j(\frac{f_i}{1}) \notin \mathfrak{p}\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} B_j : f_i \notin f(\mathfrak{p})\} \\ &= f^{-1}(\mathrm{D}(f_i)) \cap f^{-1}(\mathrm{D}(f_j)), \end{aligned}$$

thus

$$\begin{aligned} Y_{g_i} &= Y_{g_i} \cap Y = Y_{g_i} \bigcap \Big(\bigcup_{j=1}^n f^{-1}(\mathrm{D}(f_j)) \Big) \\ &= \bigcup_{j=1}^n \Big(Y_{g_i} \cap f^{-1}(\mathrm{D}(f_j)) \Big) = \bigcup_{j=1}^n \Big(f^{-1}(\mathrm{D}(f_i)) \cap f^{-1}(\mathrm{D}(f_j)) \Big) \\ &= f^{-1}(\mathrm{D}(f_i)) \bigcap \Big(\bigcup_{j=1}^n f^{-1}(\mathrm{D}(f_j)) \Big) = f^{-1}(\mathrm{D}(f_i)) \cap Y = f^{-1}(\mathrm{D}(f_i)). \end{aligned}$$

So $Y_{g_i} = f^{-1}(\mathrm{D}(f_i)) = \operatorname{Spec} B_i$ is affine. By Hartshorne (1977), Ch II, Ex. 2.17(b), Y is affine. This completes the proof. □

Proposition 3.3.2. *Let $Y \xrightarrow{g} Z \xrightarrow{f} X$ be morphisms of schemes such that f and the composed morphism $f \circ g$ are affine. Then g is affine.*

Proof. Let $\{U_i\}_{i \in I}$ be an open affine cover of X. Since f is affine, $f^{-1}(U_i)_{i \in I}$ is an open affine cover of Z and $\{g^{-1}\big(f^{-1}(U_i)\big) = (fg)^{-1}(U_i)\}_{i \in I}$ is an open affine cover of Y by assumption that fg is affine. Hence $Y \xrightarrow{g} Z$ is an affine morphism. □

Recall that a morphism $f : Y \to X$ of schemes is *finite* if there exists a covering of X by open affine subsets $U_i = \operatorname{Spec} A_i$, such that for each i, $f^{-1}(U_i)$ is affine, equal to $\operatorname{Spec} B_i$, where B_i is an A_i-algebra which is finitely generated as an A_i-module (see Hartshorne (1977) Ch II, section 3). Then finite morphisms are affine.

Definition 3.3.2. Let $f : Y \to X$ be a morphism of schemes. We call f is *finite and locally free* if there exists a covering of X by open affine subsets $U_i = \operatorname{Spec} A_i$, such that for each i, $f^{-1}(U_i) = \operatorname{Spec} B_i$ is affine, where B_i is a A_i-algebra which is finitely generated and free as an A_i-module.

From the above definition we can see that a finite and locally free morphism is affine. Similarly, we have the following:

Proposition 3.3.3. *Let $f : Y \to X$ be a morphism of schemes. Then f is finite and locally free if and only if for each open affine subset $U = \operatorname{Spec} A$ of X, the open subscheme $f^{-1}(U)$ is affine, equal to* $\operatorname{Spec} B$, *where B is a finite projective A-algebra.*

Proof. Then "if" part is clear from Theorem 3.1.1 (iv). For the "only if" part, assume f is finite and locally free, and let $U = \operatorname{Spec} A$ be an open affine subset of X. Then $f^{-1}(U)$ is affine since f is affine. Let $f^{-1}(U) = \operatorname{Spec} B$ for some A-algebra B. Then there exists a covering of U by open affine subsets $\{U_i = \operatorname{Spec} A_{f_i}\}_{i\in I}$ such that $f^{-1}(U_i) = \operatorname{Spec} B_{f_i}$ is affine for each i, where B_{f_i} is a A_{f_i}-algebra which is finitely generated and free as an A_{f_i}-module (see the proof of Hartshorne (1977), Ch II, Proposiiton 3.2). Then by Theorem 3.1.1 (iv), B is a finite projective A-algebra. This completes the proof. $\square$

Let $f : Y \to X$ be a finite and locally free morphism of schemes. Let $U = \operatorname{Spec} A$ be an open affine subset of X. Then we have $f^{-1}(U) = \operatorname{Spec} B$ with B is finite projective over A. There is a continuous rank function $[B : A] : U = \operatorname{Spec} A \longrightarrow \mathbb{Z}$, see Definition 3.1.4. Clearly, these functions defined on different U's agree on their intersections, so we can glue them to obtain a continuous function $[Y : X] : X \longrightarrow \mathbb{Z}$, where $[Y : X]|_U = [B : A]$. This function is called *degree* of Y over X, or of f, and denoted by $[Y : X]$ or $\deg(f)$. Similar as in Section 3.1, we consider $[Y : X]$ as a function between topological spaces. For each integer n the set $\{x \in \operatorname{sp}(X) \ : \ [Y : X](x) = n\}$ is open and closed in X, where $\operatorname{sp}(X)$ denotes the underlying topological space of X. Moreover, if X is connected, $[Y : X]$ is constant.

Definition 3.3.3. A morphism $Y \to X$ of schemes is called *surjective* if the map of the underlying topological spaces is surjective.

Proposition 3.3.4. *Let $f : Y \to X$ be a finite and locally free morphism of schemes. Then we have:*

(a) $Y = \emptyset \Longleftrightarrow [Y : X] = 0$.

(b) f *is an isomorphism* $\Longleftrightarrow [Y : X] = 1$.

(c) The following three assertions are equivalent:

(i) f *is surjective;*

(ii) $[Y : X] \geq 1$*;*

(iii) for every open affine subset $U = \operatorname{Spec} A$ of X, we have $f^{-1}(U) = \operatorname{Spec} B$, where B is a faithfully projective A-algebra.

Proof. We may assume that $X = \operatorname{Spec} A$ is affine. Then $Y = \operatorname{Spec} B$ for some finite projective A-algebra B. Now (a) is trivial since $Y = \emptyset \Leftrightarrow B = 0 \Leftrightarrow [B : A] = 0$. For (b), $\operatorname{Spec} B \to \operatorname{Spec} A$ is an isomorphism $\Leftrightarrow$ the induced map $A \to B$ is an isomorphism $\Leftrightarrow [B : A] = 1$ by Proposition 3.1.8. For (c), we know that $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective $\Leftrightarrow B$ is a faithfully flat A-algebra (Prop. 3.1.9) $\Leftrightarrow B$ is faithfully projective (Prop. 3.1.4) $\Leftrightarrow [B : A] \geq 1$. This completes the proof. $\square$

Definition 3.3.4. Let $f : Y \to X$ be a morphism of schemes. f is called *finite étale* if there exists a covering of X by open affine subsets $U_i = \operatorname{Spec} A_i$, such that for each i, $f^{-1}(U_i) = \operatorname{Spec} B_i$ is affine, where B_i is a free separable A_i-algebra. In this case we also say that $f : Y \to X$ is a *finite étale covering* of X.

We can easily see that a finite étale morphism is finite and locally free. Furthermore, we have an equivalent definition:

Proposition 3.3.5. *A morphism $f : Y \to X$ is finite étale if and only if for each open affine subset $U = \operatorname{Spec} A$ of X, the open subscheme $f^{-1}(U)$ of Y is affine, equal to $\operatorname{Spec} B$, where B is a projective separable A-algebra.*

The proof of this proposition is similar to the proof of Proposition 3.3.3. Just notice that the map $\psi : B \to \operatorname{Hom}_A(B, A)$ defined in Section 3.2 is an isomorphism if and only if the induced map $B_{\mathfrak{p}} \to \operatorname{Hom}_{A_{\mathfrak{p}}}(B_{\mathfrak{p}}, A_{\mathfrak{p}})$ is an isomorphism for each $\mathfrak{p} \in \operatorname{Spec} A$ and the fact that $B_{\mathfrak{p}} \cong (B_f)_{\mathfrak{p}}$ for all $\mathfrak{p} \in D(f) = \{\mathfrak{p} \in \operatorname{Spec} A : f \notin \mathfrak{p}\}$, where $f \in A$.

3.4 Properties of finite étale morphisms

Proposition 3.4.1. *Let $f_i : Y_i \to X$ be morphisms of schemes, for $1 \leq i \leq n$, and $f : Y = Y_1 \amalg Y_2 \amalg \cdots \amalg Y_n \longrightarrow X$ the induced morphism. Then f is finite and locally free (resp. finite étale) if and only* *if each f_i is finite and locally free (resp. finite étale). Moreover, we have $[Y : X] = \sum_{i=1}^{n}[Y_i : X]$ if f_i is finite and locally free.*

Proof. Case (1): f is finite and locally free. Let $U = \operatorname{Spec} A$ be an open affine subset of X. Then $f^{-1}(U) = f_1^{-1}(U) \amalg f_2^{-1}(U) \amalg \cdots \amalg f_n^{-1}(U)$. f is finite and locally free if and only if $f^{-1}(U) = \operatorname{Spec} B$ with B a finite projective A-algebra, i.e., $B = \prod_{i=i}^{n} B_i$ is finite projective over A, where $f_i^{-1}(U) = \operatorname{Spec} B_i$. By Proposition 3.1.15, this is true if and only if B_i is finite projective over A, i.e., f_i is finite and locally free.

Case (2): f is finite étale. This follows from Proposition 3.2.2 in a similar way.

Now suppose $f : Y \to X$ is finite and locally free (note that a finite étale morphism is always finite and locally free). For any $\mathfrak{p} \in X$, there exists an affine neighborhood of $\mathfrak{p}$, say $U = \operatorname{Spec} A$ such that $f^{-1}(U) = \operatorname{Spec} B$, where $B = \prod_{i=i}^{n} B_i$ and $f_i^{-1}(U) = \operatorname{Spec} B_i$ with B_i finite projective over A. Then we have

$$[Y : X](\mathfrak{p}) = [B : A](\mathfrak{p}) = \sum_{i=i}^{n}[B_i : A](\mathfrak{p}) = \sum_{i=i}^{n}[Y_i : X](\mathfrak{p}).$$

This implies $[Y : X] = \sum_{i=1}^{n}[Y_i : X]$. □

Proposition 3.4.2. *Let $(X_i)_{i\in I}$ be a collection of schemes, and $f_i : Y_i \to X_i$ be a finite and locally free (resp. finite étale) morphism, for each $i \in I$. Then the induced morphism $f : \coprod_{i\in I} Y_i \longrightarrow \coprod_{i\in I} X_i$ is finite and locally free (resp. finite étale), and each finite and locally free (resp. finite étale) morphism $\coprod_{i\in I} Y_i \longrightarrow \coprod_{i\in I} X_i$ is obtained in this way. Moreover, $[\coprod_{i\in I} Y_i : \coprod_{i\in I} X_i]\Big|_{\mathrm{sp}(X_j)} = [Y_j : X_j]$, for each $j \in I$.*

Proof. Let $\{U_{ij} = \operatorname{Spec} A_{ij}\}_{j\in J_i}$ be an open affine covering of X_i for each i. Since f_i is finite and locally free (resp. finite étale), $f_i^{-1}(U_{ij}) = \operatorname{Spec} B_{ij}$ is affine and B_{ij} is an A_{ij}-algebra that is finitely generated and free as an A_{ij}-module (resp. B_{ij} is a free separable A_{ij}-algebra). Note that $\{U_{ij}\}_{i,j}$ is an open affine cover of $\coprod_{i\in I} X_i$ and $f^{-1}(U_{ij}) = f_i^{-1}(U_{ij})$, by definition, f is finite and locally free (resp. finite étale).

Now suppose $f : Y \to \coprod_{i\in I} X_i$ is a finite and locally free (resp. finite étale) morphism. Let $Y_i = f^{-1}(X_i)$, then $Y = \coprod_{i\in I} Y_i$. For any open affine subset $U_i = \operatorname{Spec} A_i$ of X_i, U_i is also an open affine subset of $\coprod_{i\in I} X_i$. Then $f^{-1}(U_i) = \operatorname{Spec} B_i$ is an open affine subset in Y, where B_i is a finite projective (resp. separable) A_i-algebra. Furthermore, $f^{-1}(U_i) = f^{-1}(U_i) \cap Y_i$ is an open subset of Y_i. This implies the map $f_i := f|_{Y_i} : Y_i \to X_i$ is finite and locally free (resp. finite étale) by Prop. 3.3.3 (resp. Prop. 3.3.5), and f is just the map induced by f_i's.

For any $\mathfrak{p} \in X_j$, there exists an affine subset $U_j = \operatorname{Spec} A_j$ such that $\mathfrak{p} \in U_j$, $f^{-1}(U_j) = \operatorname{Spec} B_j \subseteq Y_j$ and B_j is a finite projective A_j-algebra. Then we have

$$\Big[\coprod_{i\in I} Y_i : \coprod_{i\in I} X_i\Big](\mathfrak{p}) = [B_j : A_j](\mathfrak{p}) = [Y_j : X_j](\mathfrak{p}).$$

This implies $[\coprod_{i\in I} Y_i : \coprod_{i\in I} X_i]\Big|_{\mathrm{sp}(X_j)} = [Y_j : X_j]$, for each $j \in I$. $\square$

Proposition 3.4.3. *Let $f : Y \to X$ be a finite and locally free (resp. finite étale) morphism of schemes, and let $W \to X$ be any morphism of schemes. Then*

(a) $Y \times_X W \to W$ is finite and locally free (resp. finite étale).

(b) The following diagram is commutative.

$$\begin{tikzcd} \mathrm{sp}(W) \arrow[r] \arrow[d, "{[Y\times_X W:W]}"'] & \mathrm{sp}(X) \arrow[d, "{[Y:X]}"] \\ \mathbb{Z} \arrow[r, equal] & \mathbb{Z} \end{tikzcd}$$

(c) If f is surjective, then $Y \times_X W \to W$ is surjective.

Proof. (a): Suppose we have the following commutative diagram,

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

where p_1, p_2 are the natural projections. Let $\{U_i = \operatorname{Spec} A_i\}_{i\in I}$ be an open affine covering of X and let $W_i = g^{-1}(U_i)$, $Y_i = f^{-1}(U_i)$. Since f is finite and locally free (resp. finite étale), Y_i is affine, equal to $\operatorname{Spec} B_i$, where B_i is a finite projective (resp. separable) A_i-algebra. Cover W_i by open affine subsets $\{W_{ij} = \operatorname{Spec} C_{ij}\}_{j \in J_i}$, then $\{W_{ij}\}_{i,j}$ is an open affine covering of W. Furthermore,

$$p_2^{-1}(W_{ij}) \cong Y \times_X W_{ij} \cong Y_i \times_{U_i} W_{ij} = \operatorname{Spec} B_i \times_{\operatorname{Spec} A_i} \operatorname{Spec} C_{ij} = \operatorname{Spec}(B_i \otimes_{A_i} C_{ij}).$$

(For the first two isomorphisms, see Hartshorne (1977) ChII, proof of Theorem 3.3). By Prop. 3.1.7 (resp. Prop. 3.2.4), $B_i \otimes_{A_i} C_{ij}$ is finite projective (resp. separable) over C_{ij}, which implies $p_2 : Y \times_X W \to W$ is finite and locally free (resp. finite étale).

(b) follows from Prop. 3.1.7.

(c): Suppose $f : Y \to X$ is surjective. By Prop. 3.3.4 (c), $[Y : X] \geq 1$. Then $[Y \times_X W : W] \geq 1$ by (b) thus $Y \times_X W \to W$ is also surjective. □

Proposition 3.4.4. *Suppose $g : Z \to Y$ and $f : Y \to X$ are finite and locally free (resp. finite étale) morphisms of schemes, then $f \circ g$ is finite and locally free (resp. finite étale).*

Proof. The case f is finite and locally free follows from Prop. 3.3.3 and Prop. 3.2.1. Similarly, Prop. 3.3.5 and Prop. 3.2.3 imply the case f is finite étale. □

Remark 3.4.1. In the next chapter, we will see a different proof of the case f is finite étale by a base change of a surjective, finite and locally free morphism.

Proposition 3.4.5. *Let $g : Z \to X$ and $f : Y \to X$ be finite and locally free (resp. finite étale) morphisms of schemes. Then*

(a) $Y \times_X Z \to X$ is finite and locally free (resp. finite étale).

(b) $[Y \times_X Z : X] = [Y : X] \cdot [Z : X]$.

(c) If f and g are surjective, then $Y \times_X Z \to X$ is surjective.

Proof. (a) follows from Prop. 3.4.3 and 3.4.4 immediately.

(b) is obvious since $[B \otimes_A B' : A] = [B : A] \cdot [B' : A]$ for finite projective A-algebras B and B' by Prop. 3.1.6.

(c) is clear by Prop. 3.4.3 (c) and the fact that the composite of surjective maps is surjective. $\square$

Proposition 3.4.6. *A morphism $f : Y \to X$ is surjective, finite and locally free if and only if for each open affine subset $U = \operatorname{Spec} A$ of X, the open subscheme $f^{-1}(U)$ is affine, equal to* $\operatorname{Spec} B$, *where B is a faithfully projective A-algebra.*

Proof. The "if" part is obvious and the "only if" part follows from Prop. 3.3.4 (c) immediately. $\square$

Proposition 3.4.7. *Let $f : Y \to X$ be an affine morphism of schemes, and $g : W \to X$ a morphism which 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. The "only if" part follows from Prop. 3.4.3 (a). To prove the "if" part, let $U = \operatorname{Spec} A$ be an open affine subset of X. Then $f^{-1}(U)$ is affine since f is affine. Suppose $f^{-1}(U) = \operatorname{Spec} B$ for some A-algebra B. By Prop. 3.4.6, there is a faithfully projective A-algebra C such that $g^{-1}(U) = \operatorname{Spec} C$. Moreover, we have $p_2^{-1}(g^{-1}(U)) = f^{-1}(U) \times_U g^{-1}(U) = \operatorname{Spec}(B \otimes_A C)$ (see Hartshorne (1977) ChII, proof of Theorem 3.3), where p_2 is the natural projection $Y \times_X W \to W$. Then p_2 is finite étale implies $B \otimes_A C$ is projective separable over C. From Prop. 3.2.4, B is a separable A-algebra thus f is finite étale. $\square$

A *morphism* from a finite étale covering $f : Y \to X$ to a finite étale covering $g : Z \to X$ is a morphism of schemes $h : Y \to Z$ for which the following diagram

$$\begin{tikzcd} Y \arrow[rr, "h"] \arrow[dr, "f"'] & & Z \arrow[dl, "g"] \\ & X & \end{tikzcd}$$

commutes. Then for a given scheme X, all finite étale coverings $Y \to X$ of X with morphism between them form a category and we denote this category by $\mathbf{FEt}(X)$. In the next chapter, we will show that $\mathbf{FEt}(X)$ is a Galois category if X is connected and prove our main theorem:

Theorem 3.4.1. *Let X be a connected scheme. Then there exists a profinite group π, uniquely determined up to isomorphism, such that the category* ***FEt***(X) *of finite étale coverings of X is equivalent to the category π**-sets** of finite sets on which π acts continuously.*

To end this chapter, we give an explicit description of separable algebras over algebraically closed fields, which will play an important role in the construction of the fundamental functor $F : \mathbf{FEt}(X) \to \mathbf{Sets}$ in the next chapter. We introduce a lemma first.

Lemma 3.4.1. *Let B be a finite dimensional algebra over a field K. Then $B \cong \prod_{i=1}^{t} B_i$ for some $t \in \mathbb{Z}_{\geq 0}$, where B_i is a local K-algebra with a nilpotent maximal ideal.*

Proof. We break the proof of this proposition to two cases. First we consider a simple case that B is an integral domain. Then for any $b \in B - \{0\}$, the multiplication map $m_b : B \to B$ is an injective K-algebra homomorphism, thus is an isomorphism since the dimension over K is finite. This implies that $b \in B^*$, the set of units in B. Hence B is a field, also is a finite extension of K.

Now let B be a finite K-algebra. For any $\mathfrak{p} \in \operatorname{Spec} B$, applying the above argument to $B/\mathfrak{p}$ we deduce that every prime ideal $\mathfrak{p}$ of B is maximal. Let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_s$ be distinct maximal ideals of B. By the Chinese remainder theorem the natural map $B \to \prod_{i=1}^{s}(B/\mathfrak{m}_i)$ is surjective (since distinct maximal ideals are pairwise relatively prime). So $s \leq \sum_{i=1}^{s} \dim_K(B/\mathfrak{m}_i) \leq \dim_K(B) = n$. This means that B has only finitely many maximal ideals, say $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_t$. Then we identify the kernel of the natural map $\theta : B \to \prod_{i=1}^{t}(B/\mathfrak{m}_i)$ by

$$\operatorname{Ker}(\theta) = \prod_{i=1}^{t} \mathfrak{m}_i = \bigcap_{i=1}^{t} \mathfrak{m}_i = \mathfrak{N}(B),$$

where $\mathfrak{N}(B)$ is the nilradical $\sqrt{0}$ of B. Note that B is obviously Noetherian, hence $\mathfrak{N}(B)$ is finitely generated. Then there exists an positive integer N such that $\mathfrak{N}(B)^N = \prod_{i=1}^{t} \mathfrak{m}_i^N = 0$. The $\mathfrak{m}_i$'s are pairwise relatively prime, so the same is true for the $\mathfrak{m}_i^N$'s. Then the Chinese remainder theorem gives an isomorphism $B \cong \prod_{i=1}^{t}(B/\mathfrak{m}_i^N)$. Let $B_i = B/\mathfrak{m}_i^N$, thus B_i is a local K-algebra with $\mathfrak{m}_i/\mathfrak{m}_i^N$ its only maximal ideal, which is clearly nilpotent. This proves our assertion. □

Theorem 3.4.2. *Let Ω be an algebraically closed field and B be a finite Ω-algebra. Then B is separable over Ω if and only if $B \cong \Omega^n$ as Ω-algebras, for some $n \geq 0$.*

Proof. Applying the previous lemma to B we have $B \cong \prod_{i=1}^{t} B_i$ for certain local Ω-algebras B_i with nilpotent maximal ideal $\mathfrak{m}_i$. By Prop. 3.2.2, each B_i is a separable Ω-algebra. This means that the map $\psi_i : B_i \to \mathrm{Hom}_\Omega(B_i, \Omega)$, $b \mapsto \Big(x \mapsto \mathrm{Tr}_{B/A}(bx)\Big)$ is an isomorphism for each i. Fix an i and take any $b \in \mathfrak{m}_i$. Then for any $x \in B_i$, bx is a nilpotent of B_i and the corresponding multiplication map m_{bx} is thus a nilpotent Ω-linear map. From linear algebra and Example 3.2.1 we know that $\mathrm{Tr}(bx) = 0$ for any $x \in B_i$, i.e., $\psi(b) = 0$. $b = 0$ since ψ is an isomorphism. This implies $\mathfrak{m}_i = 0$ thus B_i is a finite field extension over an algebraically closed field Ω, therefore $B_i = K$. This completes the proof. $\square$

Chapter 4

The category $\mathbf{FEt}(X)$

4.1 Totally split morphisms

Definition 4.1.1. A morphism $f : Y \to X$ of schemes is said to be *totally split* if $X = \coprod_{n\geq 0} X_n$, such that for each n, the scheme $f^{-1}(X_n) \cong X_n \amalg X_n \amalg \cdots \amalg X_n$ (n-copies), and the following diagram

$$\begin{tikzcd} f^{-1}(X_n) \arrow[r, "\cong"] \arrow[d, "f"'] & X_n \amalg \cdots \amalg X_n \arrow[d] \\ X_n \arrow[r, equal] & X_n \end{tikzcd}$$

commutes with the natural morphism $X_n \amalg \cdots \amalg X_n \to X_n$.

Remark 4.1.1. If $f : Y \to X$ is totally split, then f is finite étale since A^n is a separable A-algebra by Example 3.2.1. If X is connected, then a totally split morphism $f : Y \to X$ gives an isomorphism $Y \cong X \amalg X \amalg \cdots \amalg X$ (n copies of X), for some $n \geq 0$. Totally split morphisms play a role similar to trivial coverings in the topological case.

Proposition 4.1.1. *Let $f : Y \to X$ be a totally split morphism of schemes and $g : W \to X$ any morphism. Then the second projection $p_2 : Y \times_X W \to W$ is totally split.*

Proof. First, we assume that $[Y : X] = n$ is a constant, i.e., $Y = X \amalg \cdots \amalg X$ (n copies) and

$f : Y \to X$ coincides with the natural morphism $X \amalg \cdots \amalg X \to X$. Then

$$\begin{aligned} Y \times_X W &\cong (X \amalg \cdots \amalg X) \times_X W \\ &\cong (X \times_X W) \amalg \cdots \amalg (X \times_X W) \quad (n \text{ copies}) \\ &\cong W \amalg \cdots \amalg W \quad (n \text{ copies}), \end{aligned}$$

and the second projection $p_2 : Y \times_X W \to W$ coincides with the natural morphism $W \amalg \cdots \amalg W \to W$, so is totally split.

In general, suppose $X = \coprod_{n \geq 0} X_n$, such that for each n, the scheme $f^{-1}(X_n) \cong X_n \amalg X_n \amalg \cdots \amalg X_n$ (n-copies). Then $W = \coprod_{n \geq 0} W_n$, where $W_n = g^{-1}(X_n)$. Moreover, we have

$$\begin{aligned} p_2^{-1}(W_n) &\cong Y \times_X W_n \cong f^{-1}(X_n) \times_{X_n} W_n \\ &\cong W_n \amalg \cdots \amalg W_n \quad (n \text{ copies}) \end{aligned}$$

by the previous case. So $p_2 : Y \times_X W \to W$ is totally split. $\square$

Theorem 4.1.1. *Let $f : Y \to X$ be a morphism of schemes. Then f is finite étale if and only if f is affine and $Y \times_X W \to W$ is totally split for some $W \to X$ which is surjective, finite and locally free.*

Proof. The "if" part follows from Proposition 3.4.7 and the fact that totally split morphisms are finite étale (see Remark 4.1.1). For the other direction, let $f : Y \to X$ be finite étale. First we prove the case that $[Y : X] = n$ is constant by induction on n. When $n = 0$, $Y = \emptyset$ and $W = X \xrightarrow{\mathrm{id}_X} X$ satisfies the condition. For $n \geq 1$, note that f is surjective by Prop. 3.3.4. We make a base change by f and consider the morphism $p : Y \times_X Y \to Y$, which is also finite étale and $[Y \times_X Y : Y] = [Y : X] = n$ by Prop. 3.4.3. Let $\Delta : Y \to Y \times_X Y$ be the diagonal morphism such that $p \circ \Delta = \mathrm{id}_Y$.

Next, we claim that Δ is an open and closed immersion. First we assume $X = \operatorname{Spec} A$ for some ring A. Then $Y = \operatorname{Spec} B$, where B is a projective separable A-algebra since f is finite étale. In this case, $Y\times_X Y \cong \operatorname{Spec}(B\otimes_A B)$ and Δ corresponds to the multiplication $m : B\otimes_A B \to B$, $b\otimes b' \mapsto bb'$. By Remark 3.2.1, there exists a B-algebra C and a B-algebra isomorphism $B\otimes_A B \xrightarrow{\sim} B\times C$ such that the following diagram

$$\begin{tikzcd} B\otimes_A B \arrow[r, "\sim"] \arrow[d, "m"'] & B\times C \arrow[d, "\pi_1"] \\ B \arrow[r, equal] & B \end{tikzcd}$$

commutes, where π_1 is the natural projection. This diagram corresponds to a commutative diagram of morphisms of schemes:

$$\begin{tikzcd} Y\times_X Y \arrow[r, "\sim"] & Y \amalg \operatorname{Spec} C \\ Y \arrow[u, "\Delta"] \arrow[r, equal] & Y, \arrow[u, "j"'] \end{tikzcd}$$

where j is the inclusion morphism. So Δ is an open and closed immersion when X is affine. In general, we cover X by open affine subsets, our claim follows from the fact that f is affine. This proves the claim.

Then we obtain the following commutative diagram

$$\begin{tikzcd} Y\times_X Y \arrow[r, "\sim"] \arrow[d, "p"'] & Y \amalg Y' \arrow[d] \\ Y \arrow[r, equal] & Y \end{tikzcd}$$

by gluing together all of the local decompositions. Prop. 3.4.1 tells us that $Y' \to Y$ is finite étale and $[Y' : Y] = n-1$. Applying the inductive hypothesis, there is a surjective, finite and locally free morphism $W \to Y$ such that $Y' \times_Y W \to W$ is totally split. Since

$$\begin{aligned} Y\times_X W &\cong Y\times_X (Y\times_Y W) \cong (Y\times_X Y)\times_Y W \\ &\cong (Y\amalg Y')\times_Y W \cong (Y\times_Y W)\amalg (Y'\times_Y W) \\ &\cong W\amalg (Y'\times_Y W)\,. \end{aligned}$$

Then $Y\times_X W \to W$ is totally split since $W \to W$ and $Y'\times_Y W \to W$ are totally split. Moreover, by Prop. 3.4.3 and 3.4.4, the composite $W \to Y \to X$ is surjective, finite and locally free since each of the morphisms is. This means the theorem holds for the case $[Y : X] = n$ is constant.

In the general case, write $X = \coprod_{n=0}^{\infty} X_n$, where $\mathrm{sp}(X_n) = \{x \in \mathrm{sp}(X) : [Y : X](x) = n\}$. Then for each n, the restriction $f : Y_n = f^{-1}(X_n) \to X_n$ is finite étale of constant degree n. By the above argument, there exists a surjective, finite and locally free morphism $W_n \to X_n$ for each n, such that $Y_n \times_{X_n} W_n \to W_n$ is totally split. Then $W = \coprod_{n=0}^{\infty} W_n \longrightarrow \coprod_{n=0}^{\infty} X_n = X$ is finite and locally free and $Y \times_X W \cong \coprod_{n=0}^{\infty} (Y \times_X W_n) \cong \coprod_{n=0}^{\infty} (Y_n \times_{X_n} W_n) \to W$ by Prop. 3.4.2. This proves the theorem. $\square$

As said in Remark 3.4.1, we will give another proof of the property that the composite of finite étale morphisms is finite étale.

Proposition 4.1.2. *Let $g : Z \to Y$ and $f : Y \to X$ be finite étale morphisms of schemes. Then the composed morphism $f \circ g : Z \to X$ is finite étale.*

Proof. First assume that $Y \to X$ is totally split and $[Y : X] = n$ is constant, i.e., $Y = X \amalg \cdots \amalg X$ (n copies). Then $Z = Z_1 \amalg Z_2 \amalg \cdots \amalg Z_n$ and the composite morphism $Z \xrightarrow{g} Y \xrightarrow{f} X$ induced by finite étale morphisms $Z_i \xrightarrow{g|_{Z_i}} X \xrightarrow{\mathrm{id}_X} X$ is finite étale.

The case $Y \to X$ is totally split of non-constant degree is immediately reduced to the preceding case.

In general, as in Theorem 4.1.1, choose a surjective, finite and locally free morphism $W \to X$ such that $Y \times_X W \to W$ is totally split. Since $Z \to Y$ is finite étale, by Prop. 3.4.3 $Z \times_X W \cong Z \times_Y (Y \times_X W) \to Y \times_X W$ is finite étale. So the composition $Z \times_X W \to Y \times_X W \to W$ is finite étale. Then $Z \to X$ is finite étale by Prop. 3.4.7. $\square$

Let X be a scheme and E a finite set of cardinality n, we write $X \times E$ for the disjoint union of n copies of X, one for each element of E, i.e., if $E = \{e_1, e_2, \ldots, e_n\}$, then $X \times E := X_{e_1} \amalg X_{e_2} \amalg \cdots \amalg X_{e_n}$ with each $X_{e_i} = X$ for $i = 1, 2, \ldots, n$. We have the following property:

Lemma 4.1.1. *Given a ring A and a finite set $E = \{e_1, e_2, \ldots, e_n\}$, we define A^E to be the ring of functions $E \to A$, with pointwise addition and multiplication.*

(a) *Let X be a scheme. Then* $X \times E \cong X \times_{\operatorname{Spec}\mathbb{Z}} (\operatorname{Spec}\mathbb{Z}^E)$*.*

(b) *Let X, Y be schemes. Then there is a natural bijection between the set* $\operatorname{Mor}(X \times E, Y)$ *and the set of maps* $E \to \operatorname{Mor}(X, Y)$*.*

(c) $(\operatorname{Spec} A) \times E \cong \operatorname{Spec} A^E$*.*

(d) *Suppose A has no non-trivial idempotents and $D = \{d_1, d_2, \ldots, d_m\}$ is a finite set. Then any A-algebra homomorphism $A^E \to A^D$ is induced by a map $D \to E$.*

Proof. Suppose $|E| = n$, $E = \{e_1, e_2, \ldots, e_n\}$.

(a) The property of a morphism of schemes to be an isomorphism is a local property. We may assume $X = \operatorname{Spec} R$ for some ring R. Then it suffices to prove that $\operatorname{Spec} A \times E \cong \operatorname{Spec} A \times_{\operatorname{Spec}\mathbb{Z}} (\operatorname{Spec}\mathbb{Z}^E)$, i.e., $A \times A \times \cdots \times A \cong A \otimes_{\mathbb{Z}} \mathbb{Z}^E$. Define

$$\varphi_1 : A \otimes_{\mathbb{Z}} \mathbb{Z}^E \to A \times \cdots \times A, \qquad a \otimes f \mapsto (f(e_i) \cdot a)_{i=1}^n\,, \quad \text{and}$$
$$\varphi_2 : A \times \cdots \times A \to A \otimes_{\mathbb{Z}} \mathbb{Z}^E, \qquad (a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i \otimes g_i,$$

where $g_i(e_j) = 1$ if $i = j$ and $g_i(e_j) = 0$ otherwise. φ_1 and φ_2 are ring homomorphisms satisfying $\varphi_1 \circ \varphi_2 = \mathrm{id}_{A \times \cdots \times A}$ and $\varphi_2 \circ \varphi_1 = \mathrm{id}_{A \otimes_{\mathbb{Z}} \mathbb{Z}^E}$. This shows (a).

(b) The following two maps satisfy the requirements:

$$\begin{aligned} \varphi : \operatorname{Mor}(X \times E, Y) &\to \{\text{maps } E \to \operatorname{Mor}(X, Y)\}\,, \\ f &\mapsto (e_i \mapsto f|_{X_i = X})\,, \end{aligned}$$

$$\begin{aligned} \psi : \{\text{maps } E \to \operatorname{Mor}(X, Y)\} &\to \operatorname{Mor}(X \times E, Y), \\ (e_i \mapsto g_i) &\mapsto g, \end{aligned}$$

where $g|_{X_i = X} = g_i$.

(c) This is equivalent to show that $A \times \cdots \times A \cong A^E$ as rings. We define two maps as follows:

$$\varphi : A^E \to A \times \cdots \times A, \qquad f \mapsto (f(e_i), \ldots, f(e_n)), \quad \text{and}$$

$$\psi : A \times \cdots \times A \to A^E, \qquad (a_1, \ldots, a_n) \mapsto (e_i \mapsto a_i).$$

Now, φ and ψ are ring homomorphisms inverse to each other. This prove (c).

(d) Suppose $|D| = m$, $D = \{d_1, d_2, \ldots, d_m\}$. Define functions $f_i : E \to A$ for $i = 1, 2, \ldots, n$ as follows: $f_i(e_j) = 1$ if $i = j$, $f_i(e_j) = 0$ otherwise. Obviously, such functions are idempotents of A^E. Moreover, these f_i's are generators of A^E as an A-module which satisfy the following equalities: $\sum\limits_{i=1}^{n} f_i = 1_{A^E}$ and $f_i f_j = 0$ if $i \neq j$, for $i, j = 1, 2, \ldots, n$. Let $\varphi : A^E \to A^D$ be any homomorphism of A-algebras. Then for any fixed k, where $1 \leq k \leq m$, $\varphi(f_i)(d_k)$ is an idempotent of A for each $1 \leq i \leq n$, i.e., $\varphi(f_i)(d_k)$ is either 1_A or 0.

For a fixed k, $1 \leq k \leq m$, since $\sum\limits_{i=1}^{n} \varphi(f_i)(d_k) = \varphi\left(\sum\limits_{i=1}^{n} f_i\right)(d_k) = \varphi\left(1_{A^E}\right)(d_k) = 1_{A^D}(d_k) = 1$, at least one of the $\varphi(f_i)(d_k)$'s are 1_A when i runs from 1 to n. On the other hand, $\varphi(f_i)(d_k)\varphi(f_j)(d_k) = \varphi(f_i f_j)(d_k) = 0$, for $i \neq j$, $i, j = 1, 2, \ldots, n$, which means at most one of the $\varphi(f_i)(d_k)$'s is 1_A. So there is exactly one i, $1 \leq i \leq n$, such that $\varphi(f_i)(d_k) = 1_A$ and $\varphi(f_j)(d_k) = 0$ when $j \neq i$ for fixed $1 \leq k \leq m$. Then we can define a map $\Theta : D \to E$ sending d_k $(1 \leq k \leq m)$ to e_{i_k} such that $\varphi(f_{i_k})(d_k) = 1_A$ and $\varphi(f_j)(d_k) = 0$ when $j \neq i_k$, $1 \leq j \leq n$. By the above argument, Θ is well-defined. Moreover, we have $\varphi(f_j)(d_k) = (f_j \circ \Theta)(d_k)$, i.e., φ is induced by Θ. Indeed, we can conclude that there is a bijection between the set $\{D \to E\}$ of maps from D to E and the set $\mathrm{Hom}_A\left(A^E, A^D\right)$ of A-algebra homomorphisms.

We have completed the proof of this lemma. $\square$

Let A be a ring, D and E finite sets with a map $\phi : D \to E$. Then ϕ induces a map $\phi^* : A^E \to A^D$, defined by $f \mapsto f \circ \phi$. Furthermore, the map ϕ^* also induces a map $\phi_* : X \times D \longrightarrow X \times E$, where $X = \mathrm{Spec}\, A$. In general, if X is any scheme, we can write $X = \bigcup_{i \in I} U_i$, where $U_i = \mathrm{Spec}\, A_i$ is affine for each i. The maps $(\phi_*)_i : U_i \times D \longrightarrow U_i \times E$ induced by $\phi : D \to E$ coincide on the intersections, hence we can glue them to a morphism $\phi_* : X \times D \longrightarrow X \times E$. This morphism ϕ_* is finite étale by Prop. 3.4.1, 3.4.2 and the fact that the identity morphism $X \to X$ is finite étale.

To prove an important property of finite étale morphism, we prove the following lemma first.

Lemma 4.1.2. *Let $f : Y \to X$, $g : Z \to X$ and $h : Y \to Z$ be morphisms of schemes such that $f = g \circ h$. If f and g are totally split, then f, g and h are locally trivial. That is, for any $x \in X$, there exist an open affine neighborhood U of x in X, two finite sets D, E with a map $\phi : D \to E$ and two isomorphisms $\alpha : f^{-1}(U) \to U \times D$, $\beta : g^{-1}(U) \to U \times E$ such that the following diagram*

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

commutes, where $U \times D \to U$, $U \times E \to U$ are the first projections, and $U \times D \to U \times E$ is the morphism induced by ϕ.

Proof. For any $x \in X$, we can find an open affine neighborhood V of x such that the totally split morphisms f and g are of constant degree when they are restricted to V. Then we have $f^{-1}(V) \cong V^D$ and $g^{-1}(V) \cong V^E$ for two finite sets D and E, where $|D| = [Y : X](x)$ and $|E| = [Z : X](x)$.

Writing $V = \operatorname{Spec} A$ for some ring A, we have $V \times D \cong \operatorname{Spec}(A^D)$ and $V \times E \cong \operatorname{Spec}(A^E)$. Then $h : f^{-1}(V) \to g^{-1}(V)$ induces a map $V \times D \to V \times E$, which corresponds to a ring homomorphism $\psi : A^E \to A^D$. Localizing at x, we get a homomorphism $\psi_x : \left(A^E\right)_{\mathfrak{p}} \cong (A_{\mathfrak{p}})^E \to (A_{\mathfrak{p}})^D \cong \left(A^D\right)_{\mathfrak{p}}$, where $\mathfrak{p}$ is the prime ideal of A corresponding to x. As $A_{\mathfrak{p}}$ is local, it has no non-trivial idempotents, so the local map ψ_x is induced by a map $\phi : D \to E$ by Lemma 4.1.1 (d). Consider the homomorphism

$\phi^* : A^E \to A^D$ induced by ϕ, we have the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Hom}_A\left(A^E, A^D\right) \arrow[d] & \{D \to E\} \arrow[l] \arrow[d, leftrightarrow] \\
\left(\mathrm{Hom}_A(A^E, A^D)\right)_{\mathfrak{p}} & \mathrm{Hom}_{A_{\mathfrak{p}}}\left(A^E_{\mathfrak{p}}, A^D_{\mathfrak{p}}\right), \arrow[l, "\sim"']
\end{tikzcd}$$

where the right vertical arrow is a bijection by Lemma 4.1.1 (d) and the bottom horizontal arrow is an isomorphism since A^E is finitely presented. This implies that $\psi_x = \phi^*_x$, where ϕ^*_x is obtained by localizing ϕ^* at $\mathfrak{p}$. Then there exists an element $a \in A - \mathfrak{p}$ such that $a\psi = a\phi^*$. The open neighborhood $U = D(a)$ of x in $V = \operatorname{Spec} A$ satisfies the requirements, which proves the lemma. $\square$

Remark 4.1.2. We may generate the above lemma in the following sense: With notations as above and let $\sigma_1, \sigma_2, \ldots, \sigma_n : Y \to Z$ be morphisms such that $f = g \circ \sigma_i$ for each i. Then for any $x \in X$, there exist an open affine neighborhood $U \subseteq X$ of x, maps of finite sets $\phi_1, \phi_2, \ldots, \phi_n : D \to E$ and two isomorphisms $\alpha : f^{-1}(U) \to U \times D$, $\beta : g^{-1}(U) \to U \times E$ such that the following diagram

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

commutes for all i.

Proposition 4.1.3. *Let $f : Y \to X$ and $g : Z \to X$ be finite étale morphisms of schemes, and $h : Y \to Z$ a morphism with $f = g \circ h$. Then h is finite étale.*

Proof. By Prop. 3.4.7, it suffices to show that there is a surjective, finite and locally free morphism $W \to Z$ such that $Y \times_Z W \to W$ is finite étale. First we assume that f and g are totally split, then by the previous lemma h is finite étale since the morphism $U \times D \to U \times E$ induced by a map $D \to E$ is finite étale, as we discussed before Lemma 4.1.2.

In the general case, using Prop. 4.1.1, we choose surjective, finite and locally free morphisms $W_1 \to X$, $W_2 \to X$ such that $Y \times_X W_1 \to W_1$ and $Z \times_X W_2 \to W_2$ are totally split. Let

$W' = W_1 \times_X W_2$, then $W' \to X$ is surjective, finite and locally free by Prop. 3.4.3, 3.4.5, and $Y \times_X W' \to W'$, $Z \times_X W' \to W'$ are totally split. Hence by the case we already dealt with, $Y \times_X W' \to Z \times_X W'$ is finite étale. Letting $W = Z \times_X W'$, we have the following commutative diagram:

$$\begin{tikzcd}
Y \times_X W' \arrow[r, "\sim"] \arrow[d, "h \times \mathrm{id}_{W'}"'] & Y \times_Z (Z \times_X W') = Y \times_Z W \arrow[d, "h \times \mathrm{id}_{Z \times_X W'}"] \\
Y \times_X W' \arrow[r, "\sim"'] & Z \times_Z (Z \times_X W') = Z \times_Z W \cong W.
\end{tikzcd}$$

Then we deduce that $h : Y \to Z$ is finite étale, as $Z \times_X W \to Z$ is surjective, finite and locally free. This shows the proposition. $\square$

4.2 $\mathbf{FEt}(X)$

Given a connected scheme X, in order to prove Theorem 3.4.1, it suffices to show that the category $\mathbf{FEt}(X)$ is a Galois category. First, we will check axioms $(G1)$ to $(G3)$ for the category $\mathbf{FEt}(X)$. Then we will construct a functor $\mathbf{FEt}(X) \to \mathbf{Sets}$ and check axioms $(G4)$ to $(G6)$.

4.2.1 $(G1)$

Proposition 4.2.1. *Let X be a scheme. Then the terminal object and fiber products exist in $\boldsymbol{FEt}(X)$.*

Proof.

- The morphism $\mathrm{id}_X : X \to X$ is clearly finite étale. So $\left\{ X \xrightarrow{\mathrm{id}_X} X \right\}$ is the terminal object in $\mathbf{FEt}(X)$.

- Suppose Y, Z and W are objects in $\mathbf{FEt}(X)$ with morphisms $f : Y \to W$ and $g : Z \to W$. Then f and g are finite étale by Prop. 4.1.3. So $Y \times_W Z \to W$ is finite étale by Prop. 3.4.5, (a). It follows from Prop. 4.1.2 that the composed morphism $Y \times_W Z \to X$ is finite étale, i.e., $Y \times_W Z$ is an object in $\mathbf{FEt}(X)$. This shows that the fiber product of any two objects over a third one exists in $\mathbf{FEt}(X)$.

Thus $\mathbf{FEt}(X)$ satisfies $(G1)$. $\square$

4.2.2 $(G2)$

At the beginning of this section we will list some basic definitions and propositions for sheaves of modules. More details can be found in Hartshorne (1977), Ch II, Section 5 Sheaves of Modules.

Definition 4.2.1. Let A be a ring and let M be an A-module. We define the *sheaf associated to* M on $\operatorname{Spec} A$, denoted by $\widetilde{M}$, as follows. For each prime ideal $\mathfrak{p} \subseteq A$, let $M_{\mathfrak{p}}$ be the localization of M at $\mathfrak{p}$. For any open set $U \subseteq \operatorname{Spec} A$ we define the group $\widetilde{M}(U)$ to be the set of functions $s : U \to \coprod_{\mathfrak{p}\in U} M_{\mathfrak{p}}$ such that for each $\mathfrak{p} \in U$, $s(\mathfrak{p}) \in M_{\mathfrak{p}}$, and such that s is locally a fraction $\frac{m}{f}$ with $m \in M$ and $f \in A$. To be precise, we require that for each $\mathfrak{p} \in U$, there is a neighborhood V of $\mathfrak{p}$ in U, and there are elements $m \in M$ and $f \in A$, such that for each $\mathfrak{q} \in V$, $f \notin \mathfrak{q}$, and $s(\mathfrak{q}) = \frac{m}{f}$ in $M_{\mathfrak{q}}$. We make $\widetilde{M}$ into a sheaf by using the obvious restriction maps.

Proposition 4.2.2. *Let A be a ring, let M be an A-module, and let $\widetilde{M}$ be the sheaf on $X = \operatorname{Spec} A$ associated to M. Then:*

(a) $\widetilde{M}$ is an $\mathcal{O}_X$-module;

(b) for each $\mathfrak{p} \in X$, the stalk $\left(\widetilde{M}\right)_{\mathfrak{p}}$ of the sheaf $\widetilde{M}$ at $\mathfrak{p}$ is isomorphic to the localized module $M_{\mathfrak{p}}$;

(c) for any $f \in A$, the A_f-module $\widetilde{M}(D(f))$ is isomorphic to the localized module M_f;

(d) in particular, $\widetilde{M}(X) = M$.

Definition 4.2.2. Let $(X, \mathcal{O}_X)$ be a scheme. A sheaf of $\mathcal{O}_X$-modules $\mathscr{F}$ is *quasi-coherent* if X can be covered by open affine subsets $U_i = \operatorname{Spec} A_i$, such that for each i there is an A_i-module M_i with $\mathscr{F}\big|_{U_i} \cong \widetilde{M_i}$. We say that $\mathscr{F}$ is *coherent* if furthermore each M_i can be taken to be a finitely generated A_i-module.

Proposition 4.2.3. *Let X be a scheme. Then an $\mathcal{O}_X$-module $\mathscr{F}$ is quasi-coherent if and only if for every open affine subset $U = \operatorname{Spec} A$ of X, there is an A-module M such that $\mathscr{F}\big|_U \cong \widetilde{M}$.*

Proposition 4.2.4. *Let X be a scheme. The kernel, cokernel, and image of any morphism of quasi-coherent sheaves are quasi-coherent. Any extension of quasi-coherent sheaves is quasi-coherent.*

Let $(X, \mathcal{O}_X)$ be a scheme. We call a sheaf of $\mathcal{O}_X$-algebras $\mathscr{F}$ to be quasi-coherent if it is at the same time a quasi-coherent sheaf of $\mathcal{O}_X$-modules.

Lemma 4.2.1. *Let X be a scheme and let $\mathscr{A}$ be a quasi-coherent sheaf of $\mathcal{O}_X$-algebras. Then there exist a unique scheme Y, and a morphism $f : Y \to X$, such that for every open affine $V \subseteq X$, $f^{-1}(V) \cong \operatorname{Spec}(\mathscr{A}(V))$ (which implies that f is an affine morphism), and for every inclusion $U \hookrightarrow V$ of open affines of Y, the morphism $f^{-1}(U) \hookrightarrow f^{-1}(V)$ corresponds to the restriction homomorphism $\mathscr{A}(V) \to \mathscr{A}(U)$. The scheme Y is called* ***Spec***$(\mathscr{A})$*. Moreover, we have $\mathscr{A} \cong f_*\mathcal{O}_Y$.*

Proof. Let $\{U_i\}_{i\in I}$ be an open affine cover of X with $U_i = \operatorname{Spec} A_i$. Let $Y_i = \operatorname{Spec}(\mathscr{A}(U_i))$. Since $\mathscr{A}$ is a sheaf of $\mathcal{O}_X$-algebras, there is a ring homomorphism $A_i = \mathcal{O}_X(U_i) \to \mathscr{A}(U_i)$, which induces a morphism of schemes $f_i : Y_i \to U_i$. We shall show that these $f_i : Y_i \to U_i$'s can be glued together, along the intersections. Let $U_{ij} := U_i \cap U_j$ and $Y_{ij} = f^{-1}(U_{ij})$, then Y_{ij} is a subscheme of Y_i. Let $W = \operatorname{Spec} R$ be any open affine subset of U_{ij}. By the quasi-coherence of $\mathscr{A}$, $\mathscr{A}\big|_{U_i} \cong \widetilde{\mathscr{A}(U_i)}$, we have

$$f_i^{-1}(W) = \operatorname{Spec}\left(\mathscr{A}\big|_{U_i}(W)\right) = \operatorname{Spec}(\mathscr{A}(W)) = \operatorname{Spec}\left(\mathscr{A}\big|_{U_j}(W)\right) = f_j^{-1}(W).$$

Covering U_{ij} by such open affine W's, we get an isomorphism $\varphi_{ij} : Y_{ij} \cong Y_{ji}$. It is easy to check that these isomorphisms satisfy the Glueing Lemma (see Hartshorne (1977), Ch II, Exercise 2.12) and f_i's coincide in the intersections. Then there is a scheme Y, and a morphism $f : Y \to X$ such that f is affine. Our assertion follows from the construction of Y.

If there is a scheme Y' and $f' : Y' \to X$ with the same properties of Y, then we can define a morphism $Y \to Y'$ by gluing together isomorphisms on open affines $\operatorname{Spec}(\mathscr{A}(U))$ where U is an open affine subset of X . Then this morphism will be an isomorphism, so we see that Y is unique.

Next, we will show that $\mathscr{A} \cong f_*\mathcal{O}_Y$. Let $(U_i)_{i\in I}$ be an open affine covering of X and U any open set of X. Then we get

$$f_*\mathcal{O}_Y(U \cap U_i) \cong \mathcal{O}_Y\left(f^{-1}(U \cap U_i)\right) \cong \mathcal{O}_Y\left(\operatorname{Spec}(\mathscr{A}(U \cap U_i))\right) \cong \mathscr{A}(U \cap U_i).$$

So $f_*\mathcal{O}_Y(U) \cong \mathscr{A}(U)$ for any open subset U of X. $\square$

Lemma 4.2.2. *Let $f : Y \to X$ be an affine morphism of schemes. Then $\mathscr{A} = f_*\mathcal{O}_Y$ is a quasi-coherent sheaf of $\mathcal{O}_X$-algebras, and $Y \cong$ **Spec**$(\mathscr{A})$.*

Proof. First, we note that the corresponding morphism of sheaves $f^\sharp : \mathcal{O}_X \to f_*\mathcal{O}_Y$ makes $f_*\mathcal{O}_Y$ to be an $\mathcal{O}_X$-algebra. By Prop.4.2.3, being quasi-coherent is local on X, we may assume that $X = \operatorname{Spec} A$ is affine and then $Y = f^{-1}(X)$ is also affine, say $Y = \operatorname{Spec} B$. So $f : Y \to X$ is induced by a ring homomorphism $A \to B$, which we still denote by f. For each $a \in A$, $D(a) = \operatorname{Spec}(A_a)$ is an open affine subset of X, and

$$(f_*\mathcal{O}_Y)(D(a)) = \mathcal{O}_Y\left(f^{-1}(D(a))\right) = \mathcal{O}_Y\left(D(f(a))\right) = B_{f(a)} = B_a.$$

Hence $f_*\mathcal{O}_Y \cong \widetilde{B}$ is quasi-coherent sheaf of $\mathcal{O}_X$-algebras.

$Y \cong$ **Spec**$(\mathscr{A})$ is obtained by the uniqueness of **Spec**$(\mathscr{A})$. $\square$

For a scheme X, let **Aff**(X) denote the category of all affine morphisms $Y \to X$, a morphism from an affine morphism $f : Y \to X$ to another affine morphism $g : Z \to X$ is a morphism of schemes $h : Y \to Z$ for which $f = g \circ h$. For any morphism $h : Y \to Z$ in **Aff**(X), this corresponds to a morphism of sheaves $h^\sharp : \mathcal{O}_Z \to h_*\mathcal{O}_Y$, which will induce another morphism of sheaves $g_*\mathcal{O}_Z \to g_*(h_*\mathcal{O}_Y) = f_*\mathcal{O}_Y$. Let **QCoh**$(\mathcal{O}_X)$ denote the category whose objects are quasi-coherent sheaves of $\mathcal{O}_X$-algebras on X. Then we define a contravariant functor

$$\Gamma : \quad \mathbf{Aff}(X) \longrightarrow \mathbf{QCoh}(\mathcal{O}_X)$$

$$\begin{aligned}(f: Y \to X) &\longmapsto f_*\mathcal{O}_Y\\ (h: Y \to Z) &\longmapsto (g_*\mathcal{O}_Z \to f_*\mathcal{O}_Y).\end{aligned}$$

Lemma 4.2.3. *Γ is an anti-equivalence of categories from $\boldsymbol{Aff}(X)$ to $\boldsymbol{QCoh}(\mathcal{O}_X)$.*

Proof. This follows from lemma 4.2.1 and 4.2.2. ☐

Thanks to the above lemma, we can now construct the quotients under finite groups of automorphisms in $\mathbf{Aff}(X)$ via replacing it by the anti-equivalent category $\mathbf{QCoh}(\mathcal{O}_X)$. Let X be a scheme and $f: Y \to X$ an affine morphism. Let G be a finite subgroup of the group of automorphisms of $Y \to X$ in $\mathbf{Aff}(X)$. By the anti-equivalence we just proved in the previous lemma, Y corresponds to a quasi-coherent sheaf of $\mathcal{O}_X$-algebras, say $\mathscr{A}$, and G corresponds to a finite subgroup of $\mathrm{Aut}_{\mathcal{O}_X}(\mathscr{A})$, which acts on $\mathscr{A}$ and fixes $\mathcal{O}_X$ and which we still denote by G.

For each open subset $U \subseteq X$, we define:

$$\mathscr{A}^G(U) := (\mathscr{A}(U))^G = \left\{a \in \mathscr{A}(U) \middle| \sigma a = a, \forall \sigma \in G\right\}.$$

Note that the map $\mathcal{O}_X(U) \to \mathscr{A}(U)$ factors through $\mathscr{A}^G(U)$ since G fixes $\mathcal{O}_X$, which makes $\mathscr{A}^G(U)$ to be an $\mathcal{O}_X(U)$-algebra. Since σ is a morphism of sheaves, σ commutes with $\rho_{VU}: \mathscr{A}(V) \to \mathscr{A}(U)$ for any open sets $U \subseteq V \subseteq X$. Then for any $a \in \mathscr{A}^G(U)$, $\sigma\rho_{VU}(a) = \rho_{VU}\sigma(a) = \rho_{VU}(a) \Rightarrow \rho_{VU}(a) \in \mathscr{A}^G(U)$. So we have the following commutative diagram:

$$\begin{tikzcd} \mathscr{A}(V) \arrow[r, "\rho_{VU}"] & \mathscr{A}(U) \\ \mathscr{A}^G(V) \arrow[u, hook] \arrow[r, "\rho_{VU}"'] & \mathscr{A}^G(U). \arrow[u, hook] \end{tikzcd}$$

This makes $\mathscr{A}^G$ into a presheaf and it is easy to verify that $\mathscr{A}^G$ is actually a sheaf. We still need to show that it is quasi-coherent. Let $U \subseteq X$ be any open subset. The map $\varphi_U: \mathscr{A}(U) \to \bigoplus_{\sigma\in G} \mathscr{A}(U)$ sending a to $(\sigma a - a)_{\sigma \in G}$ is $\mathcal{O}_X(U)$-linear, and $\mathrm{Ker}(\varphi_U) = \mathscr{A}^G(U)$. It is easy to see that these φ_U's give a morphism of sheaves of $\mathcal{O}_X$-algebras, $\varphi: \mathscr{A} \to \bigoplus_{\sigma \in G} \mathscr{A}$. Then $\mathscr{A}^G = \mathrm{Ker}(\varphi)$ is quasi-coherent since both $\mathscr{A}$ and $\bigoplus\limits_{\sigma \in G} \mathscr{A}$ are quasi-coherent (Prop.4.2.4). Moreover, any morphism $\theta : \mathscr{B} \to \mathscr{A}$ of quasi-coherent sheaf of $\mathcal{O}_X$-algebras satisfying $\sigma \circ \theta = \theta$ for all $\sigma \in G$ factors uniquely via the inclusion morphism $\mathscr{A}^G \to \mathscr{A}$. Again by the anti-equivalence of categories, $\mathscr{A}^G$ corresponds to an affine morphism over X, denoted by $g : Y/G \to X$ satisfying the universal property for the quotient of $Y \to X$ under G.

For a scheme X, let $f : Y \to X$ be an affine morphism and G a finite subgroup of the group of automorphisms of $Y \to X$ in $\mathbf{Aff}(X)$. The previous argument shows that the quotient $g : Y/G \to X$ exists in $\mathbf{Aff}(X)$. From the above construction it can be easily seen that for any open set $U \subseteq X$ we have $g^{-1}(U) \cong f^{-1}(U)/G$; and if $U = \operatorname{Spec} A$ is open affine, $f^{-1}(U) = \operatorname{Spec} B$, then $g^{-1}(U) = \operatorname{Spec}(B^G)$.

Proposition 4.2.5. *Let $f : Y \to X$ be an affine morphism, G a finite group of automorphisms of $Y \to X$ in $\boldsymbol{Aff}(X)$, and $g : W \to X$ a finite locally free morphism. Then $(Y \times_X W)/G \cong (Y/G) \times_X W$ in $\boldsymbol{Aff}_W$.*

Proof. First we note that the base change $Y \times_X W \to W$ is also an affine morphism. For each $\sigma \in G$, $f \circ \sigma = f$, and we have the following commutative diagram:

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

where the morphism $Y \times_X W \to Y \times_X W$ is obtained by the universal property of the fiber product since $g \circ p_2 = f \circ p_1 = (f \circ \sigma) \circ p_1 = f \circ (\sigma \circ p_1)$, we still denote this morphism by σ. Doing the same argument to σ^{-1} yields that σ is an automorphism of $Y \times_X W \to W$ in $\mathbf{Aff}(W)$. Moreover the action of G gives a canonical action of G on $Y \times_X W \to W$, so the quotient $(Y \times_X W)/G \to W$ is well-defined. Let us denote by ρ the morphism $Y \to Y/G$ in $\mathbf{Aff}(X)$ such that $\rho \circ \sigma = \rho$ for all $\sigma \in G$. Then the morphism $h : Y \times_X W \to (Y/G) \times_X W$ induced by ρ satisfies $h \circ \sigma = g$ for all

$\sigma \in G$. By the universal property of the quotient, there exists a unique morphism

$$\phi : (Y \times_X W)/G \longrightarrow (Y/G) \times_X W.$$

We claim that ϕ is an isomorphism, which can be checked locally on the base. We may assume that $X = \operatorname{Spec} A$ is affine, then $Y = \operatorname{Spec} B$ for some A-algebra B and $W = \operatorname{Spec} C$ for some finite projective A-algebra C since f is affine and g is finite and locally free. Furthermore, the following schemes are all affine:

$$\begin{aligned} Y/G &= \operatorname{Spec}\left(B^G\right), \\ Y \times_X W &= \operatorname{Spec}\left(B \otimes_A C\right), \\ (Y \times_X W)/G &= \operatorname{Spec}\left((B \otimes_A C)^G\right), \\ (Y/G) \times_X W &= \operatorname{Spec}\left(B^G \otimes_A C\right). \end{aligned}$$

Now it suffices to show that the natural ring inclusion $B^G \otimes_A C \hookrightarrow (B \otimes_A C)^G$ is actually an isomorphism. Consider the following exact sequence of A-modules:

$$0 \longrightarrow B^G \longrightarrow B \longrightarrow \bigoplus_{\sigma \in G} B,$$

in which the last map is given by $b \mapsto (\sigma(b) - b)_{\sigma \in G}$ for each $b \in B$. Then by the flatness of C (see remark 3.1.2), it gives rise to an exact sequence:

$$0 \longrightarrow B^G \otimes_A C \longrightarrow B \otimes_A C \longrightarrow \bigoplus_{\sigma \in G} (B \otimes_A C),$$

where the last map sends $b \otimes c \in B \otimes_A C$ to $((\sigma(b) - b) \otimes c)_{\sigma \in G}$, with kernel $(B \otimes_A C)^G$. So $B^G \otimes_A C \cong (B \otimes_A C)^G$ as required. □

Proposition 4.2.6. *Let $f : Y \to X$ be a finite étale morphism and G a finite group of $\operatorname{Aut}_X(Y)$ in **FEt**(X). Then the quotient Y/G exists in **FEt**(X).*

Proof. Thanks to the previous proposition, we have seen that $g : Y/G \to X$ exists in $\mathbf{Aff}(X)$. So it suffices to show that $g : Y/G \to X$ is finite étale if $f : Y \to X$ is.

First we prove that the quotient exists in $\mathbf{Aff}(X)$ if $Y = X \times D$ for some finite set D, the action of G being induced by an action of G on D. Then for any morphism $h : X \times D \to Z$ in $\mathbf{Aff}(X)$ such that $h \circ \sigma = h$ for all $\sigma \in G$, there exists a unique morphism $X \times (D/G) \to Z$ such that the following diagram

$$\begin{tikzcd} X \times (D/G) \arrow[d, dashed] & X \times D \arrow[l] \arrow[d] \\ Z \arrow[r] & X \end{tikzcd}$$

commutes, i.e., $X \times (D/G)$ satisfies the universal property of the quotient of $X \times D$ by G, thus $Y/G = (X \times D)\big/G \cong X \times (D/G)$, then $Y/G \to X$ is finite étale.

Let us next assume that $f : Y \to X$ is totally split. For each $x \in X$, applying remark 4.1.2 when $Y = Z$, $f = g$ and $\{\sigma_1, \sigma_2, \ldots, \sigma_n\} = G$, a finite group of automorphisms of $Y \to X$ in $\mathbf{FEt}(X)$, there exists an open affine neighborhood $U \subset X$ of x such that both $f : f^{-1}(U) \to U$ and the action of G are trivial above U, that is, there exists a finite G-set D such that $f^{-1}(U) \cong U \times D$ and the action of G on $U \times D$ is induced by an action of G on D. Then by the case just dealt with, we have $(U \times D)\big/G \cong U \times (D/G)$, so $U \times (D/G) \cong f^{-1}(U)/G \cong g^{-1}(U)$, which implies that $g^{-1}(U) \to U$ is finite étale. Since we can cover X by such U's, the morphism $g : Y/G \to X$ is finite étale in this case.

In the general case we choose a surjective, finite and locally free morphism $W \to X$ for which $Y \times_X W \to W$ is totally split. Then $(Y \times_X W)\big/G \to W$ is finite étale by the result just proved, and $(Y \times_X W)/G \cong (Y/G) \times_X W$ by Prop. 4.2.5. From proposition 3.4.7 it now follows that $Y/G \to X$ is finite étale. This proves our assertion. $\square$

Proposition 4.2.7. *The category* $\boldsymbol{FEt}(X)$ *satisfies* $(G2)$.

Proof.

- It follows from Prop. 3.4.1 that finite sums exist in $\mathbf{FEt}(X)$. In particular, $\emptyset \to X$ is the initial object.
- Quotients under finite subgroups of automorphisms exist by proposition 4.2.6.

This proves our assertion. $\square$

4.2.3 (*G*3)

Proposition 4.2.8. *Let $f : Y \to X$, $g : Z \to X$ be finite étale and $h : Y \to Z$ a morphism with $f = g \circ h$. Then h is an epimorphism in $\boldsymbol{FEt}(X)$ if and only if h is surjective.*

Proof. "Only if": Suppose now h is an epimorphism in $\mathbf{FEt}(X)$. By Prop. 4.1.3, $h : Y \to Z$ is finite étale hence it is finite and locally free. So $Z_0 = \{z \in Z : [Y : Z](z) = 0\}$ is an open and closed subscheme of Z. Then the complement $Z_1 = Z - Z_0$ is also open and closed in Z and $Z = Z_0 \amalg Z_1$. Proposition 3.3.4 implies that $h^{-1}(Z_0) = \emptyset$. Thus, h factors through a finite étale morphism $h_1 : Y \to Z_1$, which is surjective since $[Y : Z_1] = [Y : Z]\Big|_{Z_1} \geq 1$. Next, we will show that $Z_0 = \emptyset$.

Let $Z' = Z_0 \amalg Z_0 \amalg Z_1$. Since $Z \to X$ is finite étale, the restrictions $Z_i \to X$ $(i = 0, 1)$ are both finite étale thus $Z' \to X$ is finite étale. It suffices to show that the two morphisms α, $\beta : Z \to Z'$ which maps Z_0 to the first and second copy of Z_0 in Z' are equal. We check this property locally. Assume $X = \operatorname{Spec} A$ is affine, hence Y, Z_0, Z_1 are all affine. We may assume $Y = \operatorname{Spec} B$, $Z_i = \operatorname{Spec} C_i$ $(i = 0, 1)$, hence $Z = \operatorname{Spec}(C_0 \times C_1)$ and $Z' = \operatorname{Spec}(C_0 \times C_0 \times C_1)$. Then the morphism $h : Y \to Z$ corresponds to a ring homomorphism $h^* : C_0 \times C_1 \to B$. This map factors through C_1:

$$h_1^* : C_1 \to B,$$

since h factors through h_1, and h_1^* is just the ring homomorphism induced by h_1. So we have $h^* = h_1^* \circ p$, where p is the projection $C_0 \times C_1 \to C_1$. Define

$$\alpha^* : C_0 \times C_0 \times C_1 \to C_0 \times C_1 \text{ by } (a, b, c) \mapsto (a, c) \text{ and}$$

$$\beta^* : C_0 \times C_0 \times C_1 \to C_0 \times C_1 \text{ by } (a, b, c) \mapsto (b, c).$$

Let α, β be the morphisms of schemes $Z \to Z'$ induced by α^*, β^*, respectively. Since $h^* \circ \alpha^* =$

$h_1^* \circ p \circ \alpha^* = h_1^* \circ p \circ \beta^* = h^* \circ \beta^*$, we have $\alpha \circ h = \beta \circ h$. Thus $\alpha = \beta$ as h is an epimorphism. Then $\alpha^* = \beta^*$, which implies that $C_0 = 0$ and thus $Z_0 = \emptyset$. So $Z = Z_1$ and h is surjective.

"If": Now suppose h is surjective and let $Z \overset{p}{\underset{q}{\rightrightarrows}} W$ be finite étale morphisms over X such that $p \circ h = q \circ h$. We need to prove $p = q$. This is a local property so we may assume X is affine, say $X = \operatorname{Spec} A$. Then Y, Z, W are all affine, say $Y = \operatorname{Spec} B$, $Z = \operatorname{Spec} C$ and $W = \operatorname{Spec} D$, then we have the following corresponding ring homomorphisms $D \overset{p^*}{\underset{q^*}{\rightrightarrows}} C \xrightarrow{h^*} B$ such that $h^* \circ p^* = h^* \circ q^*$.

$$\begin{aligned} h \text{ is surjective} \quad &\Rightarrow \quad [Y : Z] = [B : C] \geq 1. \\ &\Rightarrow \quad h^* : C \longrightarrow B \text{ is injective (Prop. 3.1.8).} \\ &\Rightarrow \quad p^* = q^* \quad \Rightarrow \quad p = q. \end{aligned}$$

So h is an epimorphism. This completes the proof. □

Proposition 4.2.9. *Let $f : Y \to X$, $g : Z \to X$ be finite étale and $h : Y \to Z$ a morphism with $f = gh$. Then h is a monomorphism in $\boldsymbol{FEt}(X)$ if and only if h is both an open immersion and a closed immersion.*

Proof. The "if" part is easy. Since an open (or closed) immersion can factor through an isomorphism with an open (or closed) subscheme, it is obviously a monomorphism.

For the "only if" part, we assume h is a monomorphism in $\mathbf{FEt}(X)$. Considering the fibre product $Y \times_Z Y$ via the morphism h, we have the following commutative diagram:

$$\begin{tikzcd} Y \times_Z Y \arrow[rr] \arrow[dr] & & Z \arrow[dl] \\ & X. & \end{tikzcd}$$

We note that $Y \times_Z Y \to Z$ and $Y \times_Z Y \to X$ are finite étale since $Y \to Z$ and $Z \to X$ are both finite étale. So $Y \times_Z Y \to Z$ is a morphism in $\mathbf{FEt}(X)$. Let p_1 and p_2 be the two projections $Y \times_Z Y \to Y$, then we have $h \circ p_1 = h \circ p_2$ by the commutativity of the following square:

$$\begin{tikzcd} Y \times_Z Y \arrow[r, "p_2"] \arrow[d, "p_1"'] & Y \arrow[d, "h"] \\ Y \arrow[r, "h"] & Z. \end{tikzcd}$$

As h is an monomorphism, then $p_1 = p_2$. We claim that p_1 is an isomorphism. In fact this is a local property so we may assume that X is affine thus Y and Z are both affine, say $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$ and $Z = \operatorname{Spec} C$ thus $Y \times_Z Y = \operatorname{Spec}(B \otimes_C B)$. Corresponding to the above square for the fibre product, we have the following commutative square of rings:

$$\begin{tikzcd} B \otimes_C B & B \arrow[l, "p_2^*"'] \\ B \arrow[u, "p_1^*"] & C, \arrow[l, "h^*"] \arrow[u, "h^*"'] \end{tikzcd}$$

where $h^* : C \to B$ is the ring homomorphism corresponding to h and p_1^*, p_2^* are the ring homomorphisms $B \to B \otimes_C B$ corresponding to p_1, p_2, which are given by $x \mapsto x \otimes 1$ and $x \mapsto 1 \otimes x$, respectively. Note the fact that $p_1^* = p_2^*$ since $p_1 = p_2$, i.e., $x \otimes 1 = 1 \otimes x$ for any $x \in B$. So for any $x, y \in B$, we have

$$p_1^*(xy) = xy \otimes 1 = (x \otimes 1)(y \otimes 1) = (x \otimes 1)(1 \otimes y) = x \otimes y.$$

This implies that p_1^* is surjective. Now let m denote the multiplicative homomorphism $B \otimes_C B \to B$ by $x \otimes y \mapsto xy$. Then $m \circ p_1^* = \mathrm{id}_B$, which means that p_1^* is injective. Then p_1^* is an isomorphism hence m is an isomorphism. Proposition 3.1.8 shows that $[B : C] \leq 1$. Extending this globally, we have $[Y : Z] \leq 1$.

Let $Z_i = \{z \in Z : [Y : Z](z) = i\}$ for $i = 0, 1$. Then $Z = Z_0 \amalg Z_1$. By Prop. 3.3.4, $h^{-1}(Z_0) = \emptyset$ and thus h factors through an isomorphism $h_1 : Y \to Z_1$. So h is both an open and closed immersion. This completes the proof. $\square$

By Proposition 3.3.4, 4.2.8 and 4.2.9 we can easily conclude the following:

Corollary 4.2.1. *Let $f : Y \to X$, $g : Z \to X$ be finite étale and $h : Y \to Z$ a morphism with $f = gh$. Then*

(a) h is an epimorphism in $\boldsymbol{FEt}(X)$ if and only if $[Y : Z] \geq 1$.

(b) h is a monomorphism in $\boldsymbol{FEt}(X)$ if and only if $[Y : Z] \leq 1$.

(c) h is an isomorphism if and only if it is both an epimorphism and a monomorphism in $\textbf{\textit{FEt}}(X)$.

Thanks to these propositions, we can check the axiom $(G3)$ now.

Proposition 4.2.10. *Let X be a scheme. Then $\textbf{\textit{FEt}}(X)$ satisfies $(G3)$.*

Proof. Suppose $h : Y \to Z$ is a morphism in $\mathbf{FEt}(X)$, i.e., we have the following commutative diagram

$$\begin{tikzcd} Y \arrow[rr, "h"] \arrow[dr] & & Z \arrow[dl] \\ & X, & \end{tikzcd}$$

where each morphism is finite étale. We will show that $h = h_2 \circ h_1$ factors as an epimorphism h_1 and a monomorphism h_2.

Let $Z_0 = \{z \in Z : [Y : Z](z) = 0\}$, $Z_1 = Z - Z_0$. Then both Z_0 and Z_1 are open and closed subschemes of Z. By Prop. 3.4.1, Z_0 and Z_1 are objects in $\mathbf{FEt}(X)$ with $Z = Z_0 \amalg Z_1$. We have seen that $h^{-1}(Z_0) = \emptyset$, so h factors:

$$\begin{tikzcd} Y \arrow[rr, "h"] \arrow[dr, "h_1"'] & & Z = Z_0 \amalg Z_1 \\ & Z_1. \arrow[ur, hook, "h_2"'] & \end{tikzcd}$$

Here, for h_2, since it is both an open immersion and a closed immersion thus is a monomorphism in $\mathbf{FEt}(X)$ (Prop. 4.2.9). For h_1, it is an epimorphism in $\mathbf{FEt}(X)$ since it has degree at least one (Prop. 4.2.1). This shows that the category $\mathbf{FEt}(X)$ satisfies axiom $(G3)$. $\square$

4.2.4 $(G4)$

Definition 4.2.3. A *geometric point* of a scheme X is a morphism $x : \operatorname{Spec} \Omega \to X$, where Ω is an algebraically closed field.

The following property shows that geometric points exist if X is non-empty, in particular if X is connected.

Proposition 4.2.11. *Let X be a scheme. Then giving a geometric point of X is equivalent to giving a point $y \in X$ together with a field homomorphism $k(y) \to \Omega$ from the residue field at y to an algebraically closed field Ω.*

Proof. Let 0 denote the only point of $\operatorname{Spec}\Omega$.

◇ Firstly, Suppose given a geometric point of X, i.e., a morphism of schemes

$$x = (f, f^\sharp) : \{0\} = \operatorname{Spec}\Omega \longrightarrow X,$$

where $f : \{0\} \to X$ is the continuous map of the underlying topological spaces, $f^\sharp : \mathcal{O}_X \to f_*\mathcal{O}_{\operatorname{Spec}\Omega}$ is the morphism of sheaves of rings with Ω an algebraically closed field. Let $y = f(0)$, then y is a point of X. Considering the stalk $\mathcal{O}_{X,y}$, we get a local morphism

$$f_0^\sharp : \mathcal{O}_{X,y} \longrightarrow \mathcal{O}_{\operatorname{Spec}\Omega,0} = \Omega.$$

Thus $\left(f_0^\sharp\right)^{-1}(0) = \mathfrak{m}_{X,y}$, where $\mathfrak{m}_{X,y}$ is the only maximal ideal of the local ring $\mathcal{O}_{X,y}$. So $f_0^\sharp$ will induce a field homomorphism $k(y) = \mathcal{O}_{X,y}/\mathfrak{m}_{X,y} \longrightarrow \Omega$ from the residue field at y to an algebraically closed field Ω.

◇ Conversely, giving a point $y \in X$ together with a field homomorphism $k(y) \to \Omega$ from the residue field at y to an algebraically closed field Ω, we define a map between topological spaces $f : \operatorname{Spec}\Omega \to X$ by $f(0) = y$. It is easy to see that f is continuous. Now for any open set $U \subseteq X$, we define a homomorphism of rings $f^\sharp(U) : \mathcal{O}_X(U) \to f_*\mathcal{O}_{\operatorname{Spec}\Omega}(U)$ as follows:

- if $y \notin U$, then $f_*\mathcal{O}_{\operatorname{Spec}\Omega}(U) = \mathcal{O}_{\operatorname{Spec}\Omega}(\emptyset) = 0$ (the zero ring), we define $f^\sharp(U)$ as the zero map;

- if $y \in U$, then $f_*\mathcal{O}_{\operatorname{Spec}\Omega}(U) = \mathcal{O}_{\operatorname{Spec}\Omega}(\operatorname{Spec}\Omega) = \Omega$, we define $f^\sharp(U)$ to be the composition

$$\mathcal{O}_X(U) \xrightarrow{\rho_y^{\mathcal{O}_X}} \mathcal{O}_{X,y} \xrightarrow{\pi} \mathcal{O}_{X,y}/\mathfrak{m}_{X,y} = k(y) \longrightarrow \Omega,$$

where $\rho_y^{\mathcal{O}_X}$ is the canonical projection $\mathcal{O}_X(U) \to \mathcal{O}_{X,y} = \varinjlim_{y \in V \subseteq X \text{ open}} \mathcal{O}_X(V)$, π is the natural projection to the quotient ring and the last map is the given field homomorphism.

It is easy to check that $f^\sharp : \mathcal{O}_X \to f_*\mathcal{O}_{\operatorname{Spec}\Omega}$ is a morphism of sheaves and $f_0^\sharp : \mathcal{O}_{X,y} \to f_*\mathcal{O}_{\operatorname{Spec}\Omega,0} = \Omega$ is local. So $x = (f, f^\sharp)$ is a morphism of schemes $\operatorname{Spec}\Omega \to X$, hence is a geometric point of X.

We complete the proof. $\square$

Remark 4.2.1. If a scheme X is non-empty (in particular, X is connected), we may take a point $x \in X$ and let Ω be the algebraic closure of $k(x)$, the residue field at x. Then x together with the field inclusion $k(x) \hookrightarrow \Omega$ gives a geometric point of X.

Now let X be a scheme and fix $x : \operatorname{Spec}\Omega \to X$ a geometric point of X over an algebraically closed field Ω. If $Y \to X$ is finite étale then so is $Y \times_X \operatorname{Spec}\Omega \to \operatorname{Spec}\Omega$. Thus $Y \times_X \operatorname{Spec}\Omega = \operatorname{Spec} K$ is affine, and K is a projective separable Ω-algebra. Since Ω is algebraically closed, Theorem 3.4.2 implies that $K \cong \Omega^n$ for some positive integer n. Then $Y \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times D$ for some finite set D with $|D| = n$. Here, D is unique up to isomorphism.

Moreover, if $h : Y \to Z$ is a morphism in $\mathbf{FEt}(X)$, then there exist finite set D and E such that $Y \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times D \cong \operatorname{Spec}\left(\Omega^D\right)$ and $Z \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times E \cong \operatorname{Spec}\left(\Omega^E\right)$, see lemma 4.1.1. Then $h \times \mathrm{id}_{\operatorname{Spec}\Omega} : Y \times_X \operatorname{Spec}\Omega \to Z \times_X \operatorname{Spec}\Omega$ will induce a morphism $\operatorname{Spec}\left(\Omega^D\right) \to \operatorname{Spec}\left(\Omega^E\right)$. Again by Lemma 4.1.1, it corresponds to a map $F_x(h) : D \to E$. Now we define

$$\begin{aligned} F_x : \quad \mathbf{FEt}(X) &\longrightarrow \mathbf{Sets} \\ (Y \to X) &\longmapsto D \\ (h : Y \to Z) &\longmapsto (F_x(h) : D \to E), \end{aligned}$$

where $Y \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times D$ and $Z \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times E$. Then it is easy to check that F_x is a (covariant) functor. We want to check that axiom $(G4)$ holds for F_x and we introduce a lemma first.

Lemma 4.2.4. *Let A be a ring and D, E, E' be finite sets. Then $A^E \otimes_{A^D} A^{E'} \cong A^{E \times_D E'}$ as A-algebras.*

Proof. It is easy to check that the following A-algebra homomorphisms are inverse to each other.

$$
\begin{aligned}
\varphi : A^E \otimes_{A^D} A^{E'} &\longrightarrow A^{E\times_D E'} \\
(f,g) &\longmapsto ((e,e')\mapsto f(e)g(e')) \text{ and} \\
\psi : A^{E\times_D E'} &\longrightarrow A^E \otimes_{A^D} A^{E'} \\
\alpha &\longmapsto \sum_{(s,t)\in E\times_D E'} \alpha(s,t) f_s \otimes g_t,
\end{aligned}
$$

where

$$
f_s(s') = \begin{cases} 1, & s' = s, \\ 0, & \text{otherwise.} \end{cases}
$$

for $s, s' \in E$ and

$$
g_t(t') = \begin{cases} 1, & t' = t, \\ 0, & \text{otherwise.} \end{cases}
$$

for $t, t' \in E'$. □

Proposition 4.2.12. *Let X be a scheme. Then the functor F_x sends the terminal object in $\textbf{\textit{FEt}}(X)$ to the terminal object in **Sets** and commutes with fiber products.*

Proof.

- Since $F_x(\mathbf{1}_{\mathbf{FEt}(X)}) = F_x(X \to X) = \{1\}$, a singleton, clearly the terminal object in **Sets**.

- Suppose Y, Z and W are objects in $\mathbf{FEt}(X)$ with morphisms $f : Y \to W$ and $g : Z \to W$. And assume $W \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times D$, $Y \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times E$ and $Z \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times E'$. Then we have

$$
\begin{aligned}
(Y \times_W Z) \times_X \operatorname{Spec}\Omega &\cong (Y \times_X \operatorname{Spec}\Omega) \times_W Z \\
&\cong (Y \times_X \operatorname{Spec}\Omega) \times_{(W\times_X \operatorname{Spec}\Omega)} (W \times_X \operatorname{Spec}\Omega) \times_W Z \\
&\cong (Y \times_X \operatorname{Spec}\Omega) \times_{(W\times_X \operatorname{Spec}\Omega)} (W \times_X \operatorname{Spec}\Omega \times_W Z)
\end{aligned}
$$

$$
\begin{aligned}
&\cong (Y \times_X \operatorname{Spec}\Omega) \times_{(W \times_X \operatorname{Spec}\Omega)} (Z \times_X \operatorname{Spec}\Omega) \\
&\cong (\operatorname{Spec}\Omega \times E) \times_{(\operatorname{Spec}\Omega \times D)} (\operatorname{Spec}\Omega \times E') \\
&\cong \operatorname{Spec}\left(\Omega^E \otimes_{\Omega^D} \Omega^{E'}\right) \cong \operatorname{Spec}\left(\Omega^{E \times_D E'}\right) \\
&\cong \operatorname{Spec}\Omega \times (E \times_D E')\,.
\end{aligned}
$$

We conclude that $(\mathbf{FEt}(X), F_x)$ satisfies $(G4)$. $\square$

4.2.5 $(G5)$

Proposition 4.2.13. *Let $f : Y \to X$ be a finite étale morphism, G a finite group of $\operatorname{Aut}_X(Y)$ in $\boldsymbol{FEt}(X)$ and $g : Z \to X$ any morphism of schemes. Then $(Y \times_X Z)/G \cong (Y/G) \times_X Z$ in $\boldsymbol{FEt}(Z)$.*

Proof. As in the proof of proposition 4.2.5, the universal property of the quotient yields a morphism:

$$\phi : (Y \times_X Z)/G \longrightarrow (Y/G) \times_X Z.$$

We claim that this is an isomorphism. We proceed this in three steps.

First we assume that $Y = X \times D$ for some finite G-set D, then the action of G on Y is induced by an action of G on D. By lemma 4.1.1(a) we have

$$
\begin{aligned}
Y \times_X Z &\cong (X \times D) \times_X Z \cong \left(X \times_{\operatorname{Spec}\mathbb{Z}} (\operatorname{Spec}\mathbb{Z}^D)\right) \times_X Z \\
&\cong (X \times_X Z) \times_{\operatorname{Spec}\mathbb{Z}} (\operatorname{Spec}\mathbb{Z}^D) \cong Z \times D.
\end{aligned}
$$

Moreover G acts on this fiber product via D in this expression. So

$$(Y \times_X Z)/G \cong (Z \times D)/G \cong Z \times (D/G) \cong (X \times (D/G)) \times_X Z \cong (Y/G) \times_X Z,$$

i.e., ϕ is an isomorphism.

Next we consider the case that $f : Y \to X$ is totally split. As we did in the proof of Prop. 4.2.6, we can cover X by open affine sets U above which both $f : Y \to X$ and the action of G are trivial, that is, we can identify $f^{-1}(U)$ with $U \times D$ for some finite set D such that the action of G on

$f^{-1}(U) \cong U \times D$ is induced by an action of G on D. Then by the case we just proved, ϕ is locally an isomorphism, thus it is an isomorphism.

Finally we deal with the general case. By Theorem 4.1.1 we may choose a surjective, finite and locally free morphism $W \to X$ such that $Y_W \to W$ is totally split; here we write $-_W$ for $- \times_X W$. Then the base change

$$Y_W \times_W Z_W \cong Y_W \times_W W \times_X Z \cong Y_W \times_X Z \longrightarrow W \times_X Z \cong Z_W$$

is also totally split. Then the above result implies that

$$(Y_W \times_W Z_W)/G \cong \big(Y_W/G\big) \times_W Z_W.$$

. Since $W \to X$ is surjective, finite and locally free, so is $Z_W \cong W_Z = W \times_X Z \to X \times_X Z \cong Z$. By proposition 4.2.5, we have

$$(Y_Z \times_Z W_Z)/G \cong \big(Y_Z/G\big) \times_Z W_Z.$$

Note that we still have

$$\begin{aligned}
(Y_Z \times_Z W_Z)/G &\cong (Y \times_X Z \times_X W)/G \cong (Y \times_X W \times_W Z \times_X W)/G \\
&\cong (Y_W \times_W Z_W)/G \cong \big(Y_W/G\big) \times_W Z_W \\
&\cong \big((Y \times_X W)/G\big) \times_W Z_W \cong (Y/G) \times_X W \times_W Z \times_X W \\
&\cong (Y/G) \times_X Z \times_X W \cong (Y/G) \times_X Z \times_Z W_Z,
\end{aligned}$$

thus we have an isomorphism:

$$\big(Y_Z/G\big) \times_Z W_Z \cong (Y/G) \times_X Z \times_Z W_Z,$$

where the isomorphism above is just the base change to W_Z of the map $\phi : (Y \times_X Z)/G \longrightarrow (Y/G) \times_X Z$. Then by Prop. 3.4.6 and 3.1.4, ϕ is also an isomorphism, which completes the proof. $\square$

Proposition 4.2.14. *Let X be a scheme and x a geometric point of X. Then the functor F_x commutes with finite sums, transforms epimorphisms to epimorphisms, and commutes with passage to the quotient by a finite group of automorphisms.*

Proof. • Let $Y_i \to X$ $(i = 1, 2, \ldots, n)$ be finite étale morphisms and suppose $Y_i \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times E_i$. Then we have

$$\begin{aligned}\left(\coprod_{i=1}^{n} Y_i\right) \times_X \operatorname{Spec}\Omega &\cong \coprod_{i=1}^{n} (Y_i \times_X \operatorname{Spec}\Omega) \cong \coprod_{i=1}^{n} (\operatorname{Spec}\Omega \times E_i) \\ &\cong \operatorname{Spec}\Omega \times \left(\coprod_{i=1}^{n} E_i\right).\end{aligned}$$

Hence $F_x\left((\coprod_{i=1}^{n} Y_i) \to X\right) = \coprod_{i=1}^{n} E_i = \coprod_{i=1}^{n} F_x(Y_i \to X)$.

• Now let $h : Y \to Z$ be an epimorphism in $\mathbf{FEt}(X)$, i.e., h is surjective. Then by Prop. 3.4.3(c), the base change

$$Y \times_X \operatorname{Spec}\Omega \cong Y \times_Z (Z \times_X \operatorname{Spec}\Omega) \longrightarrow Z \times_X \operatorname{Spec}\Omega$$

is also surjective. This is equivalent to the assertion that the map $\Omega^{F_x(Y)} \cong Y \times_X \operatorname{Spec}\Omega \to Z \times_X \operatorname{Spec}\Omega \cong \Omega^{F_x(Z)}$ induced by $F_x(h) : F_x(Y) \to F_x(Z)$ is surjective. So $F_x(h)$ must be a surjection.

• Let $Y \to X$ be a finite étale morphism, G a finite group of $\operatorname{Aut}_X(Y)$ in $\mathbf{FEt}(X)$. Using Prop. 4.2.13, we can obtain that

$$(Y \times_X \operatorname{Spec}\Omega)/G \cong (Y/G) \times_X \operatorname{Spec}\Omega \cong \operatorname{Spec}\Omega \times F_x(Y/G).$$

Moreover, we have

$$\begin{aligned}(Y \times_X \operatorname{Spec}\Omega)/G &\cong (\operatorname{Spec}\Omega \times F_x(Y))/G \cong \left(\Omega^{F_x(Y)}\right)/G \\ &\cong \operatorname{Spec}\left((\Omega^{F_x(Y)})^G\right) \cong \operatorname{Spec}\left(\Omega^{F_x(Y)/G}\right) \cong \operatorname{Spec}\Omega \times \left(F_x(Y)/G\right).\end{aligned}$$

Then we can conclude that $\operatorname{Spec}\Omega \times F_x(Y/G) \cong \operatorname{Spec}\Omega \times \left(F_x(Y)/G\right)$ thus $F_x(Y/G) \cong F_x(Y)/G$.

This proposition is equivalent to the assertion that the category $\mathbf{FEt}(X)$ with the functor F_x satisfying $(G5)$. $\square$

4.2.6 $(G6)$

Lemma 4.2.5. *Let $f : Y \to X$, $g : Z \to X$ be finite étale morphisms with $[Y : X] = [Z : X]$, and suppose that $h : Y \to Z$ is a surjective morphism with $f = gh$. Then h is an isomorphism.*

Proof. First, we assume f and g are totally split. By Proposition 4.1.2, for any $x \in X$, there exists an open affine neighborhood U of x in X such that the following diagram

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

commutes since $[Y : X] = [Z : X]$. Note that ϕ is indeed surjective since h is surjective. The finiteness of D implies ϕ is bijective, thus $h\big|_{f^{-1}(U)} : f^{-1}(U) \to g^{-1}(U)$ is an isomorphism, so is h.

In the general case we choose surjective, finite and locally free morphisms $W_1 \to X$, $W_2 \to X$ such that $Y \times_X W_1 \to W_1$ and $Z \times_X W_2 \to W_2$ are totally split. Then $W = W_1 \times_X W_2 \to X$ is also surjective, finite and locally free, and $Y \times_X W \to W$, $Z \times_X W \to W$ are totally split. Furthermore, by Prop. 3.4.3 (b), we have $[Y \times_X W : W] = [Y : X] = [Z : X] = [Z \times_X W : W]$. Applying the conclusion we got above, $h \times \mathrm{id}_W : Y \times_X W \to Z \times_X W$ is an isomorphism. Since being an isomorphism is a local property, we may assume now that $X = \operatorname{Spec} A$ affine for some ring A. Then $W = \operatorname{Spec} B$ is affine with B a faithfully projective A-algebra since $W \to X$ is surjective, finite and locally free. This implies h is an isomorphism (Prop. 3.1.4). $\square$

Proposition 4.2.15. *Let X be a connected scheme and x a geometric point of X. Then $(\boldsymbol{FEt}(X), F_x)$ satisfies $(G6)$.*

Proof. Suppose we have a morphism $h : Y \to Z$ in $\mathbf{FEt}(X)$ such that $F_x(h) : F_x(Y) \to F_x(Z)$ is an isomorphism. This implies that $[Y : X] = |F_x(Y)| = |F_x(Z)| = [Z : X]$. Factor h as in the proof of Prop. 4.2.10 into:

$$\begin{tikzcd} Y \arrow[rr, "h"] \arrow[dr, "h_1"'] & & Z = Z_0 \amalg Z_1 \\ & Z_1, \arrow[ur, hook, "h_2"'] & \end{tikzcd}$$

with h_1 surjective and $Z_0 = \{z \in Z : [Y : Z](z) = 0\}$. By Prop. 4.2.14, $F_x(Z) = F_x(Z_0) \amalg F_x(Z_1)$ and $F_x(h_1) : F_x(Y) \to F_x(Z_1)$ is surjective. Then we have:

$$\begin{tikzcd} F_x(Y) \arrow[rr, "F_x(h)"] \arrow[dr, "F_x(h_1)"'] & & F_x(Z) = F_x(Z_0) \amalg F_x(Z_1) \\ & F_x(Z_1), \arrow[ur, "F_x(h_2)"'] & \end{tikzcd}$$

where $F_x(h)$ is an isomorphism and $F_x(h_1)$ is surjective. So $F_x(Z_1) = F_x(Z)$ thus $F_x(Z_0) = \emptyset$, i.e., $[Z_0 : X] = [Z_0 \times_X \operatorname{Spec}\Omega : \operatorname{Spec}\Omega] = |F_x(Z_0)| = 0$. This implies that $Z_0 = \emptyset$ hence $Z = Z_1$, i.e., h is surjective. Then by lemma 4.2.5, h is an isomorphism. So $(G6)$ was satisfied. □

Now we may conclude that:

Theorem 4.2.1. *Let X be a connected scheme, x a geometric point of X, and $F_x : \boldsymbol{FEt}(X) \to \boldsymbol{Sets}$ as defined in Section 4.2.4. Then $(\boldsymbol{FEt}(X), F_x)$ is a Galois category.*

4.3 Fundamental group

Let us write down the main theorem for this thesis:

Theorem 4.3.1. *Let X be a connected scheme. Then there exists a profinite group π, uniquely determined up to isomorphism, such that the category $\boldsymbol{FEt}(X)$ of finite étale coverings of X is equivalent to the category π-**Sets** of finite sets on which π acts continuously.*

Proof. Since X is connected, the degree $[Y : X]$ is constant for each object $(Y \to X)$ in $\mathbf{FEt}(X)$. Then it is straightforward to verify that $\mathbf{FEt}(X)$ is an essentially small category. Theorem 2.2.1(a) and 4.2.1 imply that the category $\mathbf{FEt}(X)$ is equivalent to the category π**-Sets** for some profinite group π, if X is connected. Again by theorem 2.2.1(d), π is uniquely determined up to isomorphism.

$\square$

Let X be a connected scheme, x a geometric point of X, and $F_x : \mathbf{FEt}(X) \to \mathbf{Sets}$ as defined in 4.2.4. We write $\pi(X, x) = \mathrm{Aut}(F_x)$, called the *fundamental group of X in x*, see section 2.1.6.

Bibliography

M. A. Armstrong. *Basic Topology*. Springer-Verlag New York, Inc., 1983. 2, 18

M. F. Atiyah and I. G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley, 1994. 59

R. Hartshorne. *Algebraic Geometry*. Springer, 1977. 73, 74, 75, 76, 80, 81, 93, 94

H. Herrlich and G. E. Strecker. *Category Theory ; An Introduction*. Allyn and Bacon, Boston, 1973. 13

S. Mac Lane. *Categories for the Working Mathematician*. Springer, New York, 1998. 9

W. S. Massey. *A Basic Course in Algebraic Topology*. Springer, New York, 1991. 2, 5, 6

T. Szamuely. *Galois groups and fundamental groups*. Cambridge University Press, New York, 2009. 5, 6