UNIVERSIDAD NACIONAL DE COLOMBIA

On the section conjecture in anabelian geometry

Andrés Felipe Ríos Moreno

Universidad Nacional de Colombia
Departamento de matemáticas
Ciudad, Colombia
2020

Sobre la conjetura de secciones en geometría anabeliana

Andrés Felipe Ríos Moreno

Tesis presentada como requisito parcial para optar al título de:
MaestrÃa en Ciencias-Matemáticas

Director:
PhD. John Alexander Cruz Morales

Universidad Nacional de Colombia
Departamento de matemÃ¡ticas
BogotÃ¡, Colombia
2020

A mis padres.

And the most beautiful mansion, the one that best reflects the love of the true workman, is not the one that is bigger or higher than all the others. The most beautiful mansion is that which is a faithful reflection of the structure and beauty concealed within things.

Alexander Grothendieck

Acknowledgments

I would like to thank my advisor Alexander Cruz. Suffice to say that without his help this document have been wholly impossible. Thanks to Alex for all the patience and support that gives me along all these years, for introduce me to algebraic geometry.
Thanks to my parents, Aura and Hugo, my inexhaustible source of strength. All I can thank them for will be little.
To always be with me, thanks to Dani, for all the love, the support and for being there in the hard moments, even without you knowing.
This document could not exists without all the talks and seminars we make, for your warm affection, thanks to Nicolás, David, Sebastian, Arturo and Joel.

Abstract

In this work, we study and present in detail some ground ideas of anabelian geometry, from its origin in number field and arithmetic results to the statements proposed by Grothendieck, studying theory of fundamental groups in algebraic geometry. We do emphasis in study of section conjecture.

Keywords: Anabelian geometry, Section conjecture, Galois theory, Fundamental groups, Arithmetic geometry.

Resumen

En este trabajo estudiamos y presentamos en detalle algunas ideas de geometría anabeliana, desde su origen en teoría de cuerpos y aritmética a los enunciados propuestos Grothendieck, estudiando la teoría de grupos fundamentales en geometría algebraica. Hacemos énfasis en estudiar la conjetura de secciones.

Palabras clave: Geometría anabeliana, Conjetura de secciones, Teoría de Galois, grupos fundamentales, Geometría aritmética.

Table of contents

1 Introduction

Galois theory begins with the study of solubility of polynomial equations in one variable using permutations, in modern language, provides a relation between field theory and group theory, we can study some properties of a field extension by looking at their associated Galois group. Galois theory has proven to be a common point of several theories, have analogues and applications in many areas of mathematics, for example, it gives powerful connections between algebra and arithmetic, specially in algebraic number theory. Alexander Grothendieck in [9] gave a geometric character to Galois theory in a deep extension of it to algebraic geometry. The heart of this extensions are étale morphisms, they build a common scene where topology, arithmetic and geometry have a conversation.

Nowadays Galois theory still alive in a variety of mathematical contexts, for example, Esquisse d'un programme [8] is a research program proposed by Alexander Grothendieck in 1984 in which he suggests some relations between arithmetic and geometry, as a plan of future research in mathematics, most of these themes are active research topics to this day. One part of this program is devoted to develop connections between Galois theory and geometry, for example, Dessins d'enfants, Grothendieck-teichmuller theory and anabelian geometry.

In this text we focus on anabelian geometry, roughly speaking, this theory tries to make a picture of schemes characterized by its fundamental group. Anabelian geometry has its roots in three big theorems, historically, the first one is Artin-Schreier theorem which gives a Galois description of the real closed fields, the second one is Neukirch theorem which can be understood as a p-adic analogue to Artin-Schreier theorem and it has the following nice implication: every isomorphism between the absolute Galois groups of two number fields implies a local correspondence between its primes and this correspondence gives rise to a Galois characterization of number fields, this is the third theorem due to Neukirch and Uchida. In the framework of Esquisse d'un programme the last theorem can be re stament saying that the spectrum of a number field is an example of an anabelian scheme. Grothendieck proposed other examples of anabelian schemes, namely , finitely generated fields over the rational numbers and hyperbolic curves defined over finitely generated fields, and it was only conjectures until works by Pop, Tamagawa, Mochizuki and many others, prove most of this conjectures.

Not all of Grothendieck's conjectural picture of Anabelian geometry has been full explain, remains open one mysterious conjecture, namely the section conjecture, its first appearance in literature was in a letter from Grothendieck to Faltings [7] and predicts a correspondence between k-rational points of hyperbolic curves over a finitely generated fields and sections of

the exact homotopy sequence of this curves, however, it is not too much known about this conjecture. Some experts expects that it has relation with Mordell's conjeture (now Faltings theorem).

Most ideas and results of anabelian geometry are fragmented in literature. One aim of this text is to present and unify notions of this program in a coherent way, with emphasis on the section conjecture. We divide this work in three chapters: In chapter 1 we study with some detail the proof of Artin-Schreier theorem following [13], this proof only involves basic language of fields, then we study some basic concepts and results of algebraic number theory without proofs, the main references for this part are [22] ,[23] and [21]. Following [38] we present consequences of Chebotarev's density theorem, specially, a description of finite Galois extensions of a number field in terms of factorisation of primes. A similar treatment of Neukirch's theorem,we do not present its proof, which requires cohomology of number fields, instead, we deduce the local correspondence theorem and, using these ideas, we study the proof of Galois characterizations of number fields, the main reference of this part is [37].

In chapter 2, we recall some concepts of algebraic topology about fundamental groups and covering spaces, in particular, we state a characterisation of the fundamental group of some spaces, as the automorphism group of certain functor, this gives us an idea of how define an analogue to fundamental groups in algebraic geometry. Following [24] we introduce étale morphisms, examples and properties are given. Also, in this chapter we study finite étale coverings of a scheme and we present useful results that are quite similar to properties of covering spaces. We present the definition of the étale fundamental group of a scheme, as the automorphism group of certain functor, we present examples and theorems. To conclude this chapter, we study Grothendieck's geometrization of Galois theory and we deduce as a corollary the main theorem of Grothendieck-Galois theory, the main reference is [55].

Finally, in chapter 3, we introduce concrete definitions and theorems in Anabelian geometry and we mention some ideas of its proofs. We should mention that only the original Anabelian program of Grothendieck is covered here, we do not mention variants of this program like sub p-adic variant, mono-anabelian geometry, etc. In order to prove the exactness of the homotopy sequence, we present characterisations of surjectivity and injectivity of homomorphisms induced by étale fundamental group functors, our main reference is [55] but some proofs are modified in this text. Finally, following [54] we state Grothendieck's section conjecture, we study descriptions of sections of exact sequences of groups in terms of non-abelian cohomology and torsors, we use this characterisation and results of abelian varieties to derive the injectivity of the profinite Kummer map for projective curves of genus at least zero over finitely generated fields.

2 Pre-anabelian geometry

In this chapter we introduce the absolute Galois group of a field. We investigate what kind of information a field are codified in its absolute Galois group, first for real closed fields and then for number fields. We study some arithmetic properties of number fields codified in the Galois absolute group of these fields, we study how a p-adic variant to Artin-Schreier theorem, namely the Neukirch, implies a local correspondence between primes and finally the Galois characterization of number fields. We finally this chapter with a characterization of the automorphism group of the rational numbers.

2.1 The Artin-Schreier theorem

Let k be a field, we fix an algebraic closure $\overline{k}$ of k, and we denote by k^{sep} the separable closure of k inside $\overline{k}$.
For an extension L of k, we denote by $Aut(L|k)$ the group of automorphisms of L that fixes pointwise k. If in addition, L is a Galois extension of k, the group $Aut(L|k)$ is denoted by $Gal(L|k)$. $\overline{k}$ is not, in general, a Galois extension of k, while k^{sep} is always a Galois extension of k, but the automorphisms groups associated to this two extensions are isomorphic. Indeed, the inclusion $k^{sep} \to \overline{k}$ induces an isomorphism $Aut(\overline{k}|k) \to Aut(k^{sep}|k) = Gal(k^{sep}|k)$.

Definition 2.1.1. *The **absolute Galois group** of k is the group $Gal(k^{sep}|k)$, we denote this group by Gal_k.*

Let L be Galois extension of k (not necessary a finite extension of k). The Galois group $Gal(L|k)$ can be approximated by the finite finite Galois extensions intermediate to L and k. To be precise, denote by G_k^L be the directed set of intermediate extension of k and L, that are finite and Galois over k. Then we have the next isomorphism

$$Gal(L|k) \simeq \varprojlim_{M \in G_l^L} Gal(M|k).$$

As M is a finite extension of k, then $Gal(M|k)$ is a finite group and therefore $Gal(L|k)$ is a profinite group. In particular, the absolute Galois group of every field is profinite.

What kind of information Gal_k codifies about k?

Galois theory states that the closed subgroups of Gal_k (with the profinite topology) are in bijection with the separable extensions of k. Then, Gal_k codifies the lattice of separable extensions of k as the lattice of his closed subgroups.
Unfortunately, Gal_k does not codifies the isomorphy type of k. For example, if k is a finite field and M is finite extension of k, then $Gal(M|k)$ is a cyclic finite group generated by the Frobenius automorphism, and therefore $Gal(M|k) \simeq \mathbb{Z}/n\mathbb{Z}$, where n is the degree of M over k. Reciprocally, if $n \in \mathbb{Z}^+$, then there exists a finite extension M of degree n over k and therefore $\mathbb{Z}/n\mathbb{Z}$ occurs as the Galois group of some finite extension of k. Thus,

$$Gal_k \simeq \varprojlim_{n\in\mathbb{Z}^+} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}},$$

where $\hat{\mathbb{Z}}$ is the group of profinite integers. This example shows that every two finite fields have isomorphic absolute Galois groups. In particular, the absolute Galois group of a field does not codifies the isomorphy type of k.
Recall that an algebraic closure of the field of real number $\mathbb{R}$ is the quadratic extension of the complex numbers $\mathbb{C}$, and therefore absolute Galois group of $\mathbb{R}$ is a group of order two (thus isomorphic to $\mathbb{Z}/2\mathbb{Z}$), generated by the complex conjugation. As we seen before, there at least two non isomorphic fields with absolute Galois group isomorphic to the group of profinite integers, is the same true for $\mathbb{Z}/2\mathbb{Z}$?
To answer, consider the algebraic closure $\overline{\mathbb{Q}}$ of the rational numbers, embedded in the field of the complex numbers. The field of real algebraic numbers is the field defined by $\mathbb{R}^{alg} = \overline{\mathbb{Q}} \cap \mathbb{R}$ (this intersection is a subset of $\mathbb{C}$). Consider the subfield of the complex numbers, defined by

$$l = \{a + ib | a, b \in \mathbb{R}^{alg}\}.$$

We want to show that $l = \overline{\mathbb{R}^{alg}}$.
It is clear that l is an quadratic extension of $\mathbb{R}^{alg}$, then $l \subseteq \overline{\mathbb{R}^{alg}}$.
If $p(x)$ is a non constant polynomial over $\mathbb{R}^{alg}$ (in particular, its coefficients are real numbers), then by the fundamental theorem of the algebra there exists a complex number $\alpha = a + ib$, where $a, b \in \mathbb{R}$, such that $p(a + ib) = 0$. Consider the finite field extension $\mathbb{R}^{alg}(\alpha)$, it is not difficult to show that $a, b \in \mathbb{R}^{alg}(\alpha)$, and therefore a, b are real algebraic numbers ($\mathbb{R}^{alg}(\alpha)$ is an algebraic extension of $\mathbb{Q}$). Therefore, every zeroes of a non constant polynomial of $\mathbb{R}^{alg}$ is an element of l, i.e., $\overline{\mathbb{R}^{alg}} \subseteq l$.
Then, the algebraic closure of the field of the real algebraic numbers is a quadratic extension, therefore $Gal_{\mathbb{R}^{alg}}$ has order two, in other words, it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, but $\mathbb{R}^{alg}$ is not isomorphic to $\mathbb{R}$, because $\mathbb{R}^{alg}$ is countable.

Definition 2.1.2. *A field k is said to be* ***real closed*** *if k is not algebraically closed, but $k(i) := k[x]/\langle x^2 + 1\rangle$ is an algebraic closure of k.*

By definition, the algebraic closure of every real closed field is a quadratic extension, therefore the absolute Galois group of every real closed field is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. This special types of fields has a interesting property in terms of his absolute Galois group, they are finite. There exists other type of fields with a finite absolute Galois group? The answer to this question is yes, for example, the absolute Galois group of every algebraically closed field is trivial. So, by the moment we know that the finite groups being the absolute Galois groups of some field are two, the trivial group and $\mathbb{Z}/2\mathbb{Z}$. Which are the finite groups that are the absolute Galois group of some field? Before we ask this question, we study the Galois group of some cyclotomic extensions of the prime fields, first for the finite fields $\mathbb{F}_p$ and then for the field of rational numbers $\mathbb{Q}$.

Proposition 2.1.1. *Let $m \in \mathbb{Z}^+$ and denote by $\mathbb{F}_p(\zeta)$ m-th cyclotomic field over $\mathbb{F}_p$. The group $Gal(\mathbb{F}_p(\zeta)|\mathbb{F}_p)$ is cyclic.*

Proof. The field $\mathbb{F}_p(\zeta)$ is finite extension of $\mathbb{F}_p$, then $\mathbb{F}_p(\zeta)$ is a finite field and therefore $Gal(\mathbb{F}_p(\zeta)|\mathbb{F}_p)$ is generated by the Frobenius automorphism of this field. □

Proposition 2.1.2. *Let $e \in \mathbb{Z}^+$ and $m = p^e$ with p a prime number and let $\mathbb{Q}(\zeta)$ be the $m-th$ cyclotomic field over $\mathbb{Q}$. The group $Gal(\mathbb{Q}(\zeta)|\mathbb{Q})$ is cyclic if, and only if $p \neq 2$ and $e < 3$.*

Proof. We sketch the proof of this theorem. $Gal(\mathbb{Q}(\zeta)|\mathbb{Q})$ is isomorphic to the group $(\mathbb{Z}/m\mathbb{Z})^*$, this group is always cyclic when m is odd (when p is odd) and for m even (when $p = 2$) is cyclic if and only if $e = 1$ or $e = 2$. □

Theorem 2.1.1. ***(Artin-Schreier)*** *Let k be a field. If Gal_k is finite and no trivial, then k is a real closed field. In particular, $Gal_k \simeq \mathbb{Z}/2\mathbb{Z}$.*

Proof. We divide the proof in several steps. Let $k_1 = k(i)$, we want to show that $\overline{k} = k_1$.

(i) As k_1 is algebraic over k, then we can suppose that $k_1 \leq \overline{k}$ (if not, then we can find a ring homomorphism $k_1 \to \overline{k}$, and the image of this ring homomorphism is a subfield of $\overline{k}$ isomorphic to k_1). So, we have the next tower of fields

$$\begin{array}{c} \overline{k} \\ | \\ k_1 \\ | \\ k \end{array}$$

(ii) k_1 is perfect (that is every algebraic extension of k_1 is separable): If l is an algebraic extension of k, then we can suppose that (as in the previous step) that $l \leq \overline{k}$, then by considering the tower of fields

$$\begin{array}{c} \overline{k} \\ | \\ l \\ | \\ k \end{array}$$

we have that $[\overline{k} : k] = [\overline{k} : l][l : k]$, in particular, $[l : k] \leq [\overline{k} : k]$. In other words, $[\overline{k} : k]$ is a bound for the degree of every algebraic extension of k. Suppose that k_1 is not perfect, then $char(k_1) = p > 0$ and there exists $\beta \in k_1$, such that $\beta \notin Im(Frob_p)$, where

$$\begin{array}{rcl} Frob_p : k_1 & \rightarrow & k_1 \\ x & \rightarrow & x^p \end{array}$$

is the frobenius endomorphism of k_1. For every $e \in \mathbb{Z}^+$, consider the irreducible polynomial $\varphi_e(x) = x^{p^e} - \beta$ (this polynomial is irreducible, since $\beta \notin Im(Frob_p)$). Therefore, for every $e \in \mathbb{Z}^+$, we can construct the finite extension of k, $k[x]/\langle \varphi_e(x) \rangle$ of degree p^e over k, which contradicts the fact that the degree of every algebraic extension is bounded by the natural number $[\overline{k} : k]$ (the degree of $\overline{k}$ over k is finite, because Gal_k is a finite group). Thus, k_1 is perfect.

As k_1 is perfect, then $\overline{k}$ is a Galois extension of k_1 (an algebraically closed field is always a normal extension of any field). In the next steps we show that $Gal(\overline{k}|k_1)$ is the trivial group, this is equivalent to show that $\overline{k} = k_1$. Assume that $|Gal(\overline{k}|k_1)| > 1$.

(iii) Since $|Gal(\overline{k}|k_1)| > 1$, then there exists a prime number q and a subgroup H of $Gal(\overline{k}|k_1)$, of order q. By Galois theory, there exists an extension E of k_1, such that $[\overline{k} : E] = q$. Therefore we have the next tower of fields

$$\begin{array}{c} \overline{k} \\ | \\ E \\ | \\ k_1 \\ | \\ k \end{array}$$

as the degree of $\overline{k}$ over E is a prime number, there no exists intermediate extension between E and k.

(iv) $char(\overline{k}) \neq q$: If $char(\overline{k}) = q$, thus we have that $char(E) = q$. Therefore, for every $m \in \mathbb{Z}^*$, exists E_m a finite extensions of E of degree q^m , in particular E_m are algebraic extensions of k with degree at least q^m, this contradicts the fact that there exists a bound for the degree of every algebraic extension (as we shown in the second step).

(v) $\overline{k}$ contains exactly q distinct q-roots of the unity: Let $f(x) = x^q - 1$, as $char(\overline{k}) \neq q$, then the polynomial $f(x)$ is separable (provided that if α is a zero of f, then $f^{'}(\alpha) = q(\alpha)^{q-1} \neq 0$) and the coefficients of f are in k, then every root of f is in $\overline{k}$.

(vi) $\overline{k} = E(\sqrt[q]{\alpha})$: Consider the polynomial $f(x) = x^q - 1$, f has a root in E (the root 1), in particular f is not irreducible over E. If $g(x)$ is an irreducible factor of f in E, then $E^{'} = E[x]/\langle g(x)\rangle$ is an intermediate extension between E and $\overline{k}$, therefore $E^{'} = E$ or $E^{'} = \overline{k}$. If $E^{'} = \overline{k}$, in particular, $[E^{'} : k] = q$, but this contradicts the fact that $deg(g) < deg(f) = q$. Therefore $E^{'} = E$, i. e., $deg(g) = 1$ this means that the polynomial f splits completely in E. Thus by $\overline{k} = E(\sqrt[q]{\alpha})$, for some $\alpha \in E$.

Let $\rho \in \overline{k}$ such that $\rho^{q^2} = \alpha$ and consider the polynomial

$$g(x) = \prod_{i=1}^{q^2}(x - \zeta^i\rho),$$

where ζ is a primitive q^2- root of the unity. Note that $g(x) = x^{p^2} - \alpha$, therefore g is a polynomial in $E[x]$.

(vii) For every $i \in 1, ..., q^2$, $\zeta^i\rho \notin E$. Because if $\zeta^i\rho \in E$, then $\beta = (\zeta^i\rho)^q \in E$. But

$$\begin{aligned} \beta^q &= ((\zeta^i\rho)^q)^q \\ &= (\zeta^{qi}\rho^{q^2}) \\ &= 1.\alpha \\ &= \alpha \end{aligned}$$

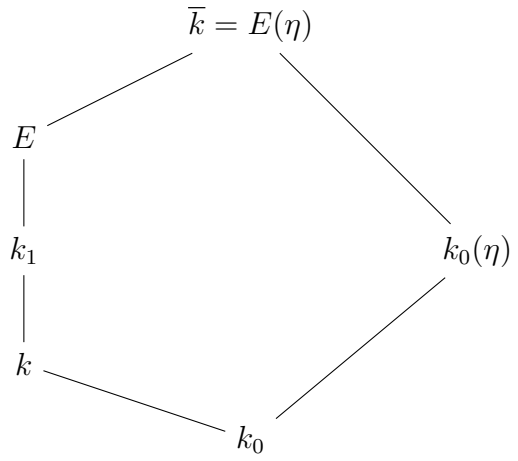
i.e. β, a q-root of α, is an element of E. Thus, $E = \overline{k}$, a contradiction.

(viii) As the roots of the polynomial g are not elements of E, then the irreducible components of g over E are of degree q. Let γ be the constant element of one of the irreducible components of g. We can write $\gamma = \rho^q\eta$, where η is a power of ζ. $\rho^q \notin E$ (because $(\rho^q)^q = \alpha$), then we can write $\overline{k} = E(\rho^q)$, but as $\gamma \in E$,then we have

$$\overline{k} = E(\rho^q) = E(\gamma\rho^{-q}) = E(\eta),$$

in particular this implies that $\eta \notin E$, since η is a q^2-root of the unity and E contains all the $q - root$ of the unity, then η is a primitive q^2-root of the unity.

(ix) Let k_0 be the prime field of $\overline{k}$ (is the same prime field of $\overline{k}$). If we consider the field $k_0(\eta)$, we have the next diagram of fields and inclusions



is possible find a natural number r and a primitive q^{r+1}-root of the unity ϵ such that $\epsilon \in \overline{k} \setminus k_0(\eta)$. Indeed,

(a) If $k_0 = \mathbb{Q}$, then for every $s \in \mathbb{Z}^+$ the field extension k_s of q^s-roots of the unity has degree $\varphi(q^s)$ over $\mathbb{Q}$ (here φ is the Euler function).

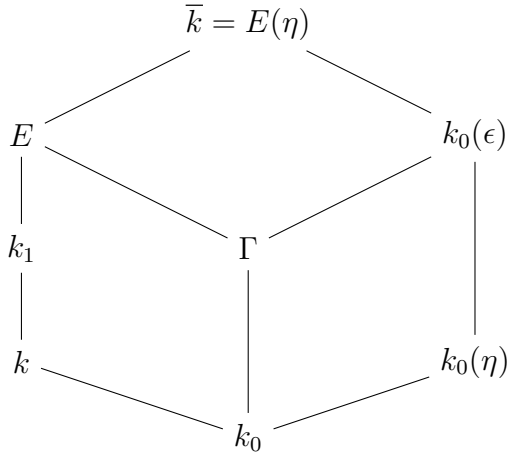
(b) If $k_0 = \mathbb{F}_p$, for a prime number $p \neq q$, then the field extension k_s of q^s-roots of the unity has degree at least q^s.

In any case $\lim_{s\to\infty}[k_s : k_0] = \infty$, as $k_0(\eta)$ is a finite extension of k_0, then the assertion follows.

Let ϵ be a primitive q^{r+1}-root of unity such that $\epsilon \in \overline{k} \setminus k_0(\eta)$ (In particular, $r \geq 2$).

(x) $\epsilon \notin E$. Indeed, as ϵ is a primitive p^{r+1}-root of the unity, then there exists $n \in \mathbb{Z}^+$, such that $\epsilon^n = \eta$ (η is a q^2-root of the unity, in particular, a q^{r+1}-root of the unity), so is impossible that $\epsilon \in E$. Let $h(x)$ be the irreducible polynomial of ϵ over E, as $[\overline{k} : E] = q$ with q prime and $\epsilon \notin E$, then h has degree q. Is clear that $h(x)$ is a factor of the polynomial $x^{q^{r+1}} - 1 = \prod_{i=1}^{q^{r+1}}(x - \epsilon^i)$, then all the coefficients of h are powers of ϵ, in particular, $h(x) \in k_0(\eta)[x]$.

If we denote by $\Gamma = E \cap k_0(\epsilon)$. We have the next diagram of fields and inclusions



(xi) $[k_0(\epsilon) : \Gamma] = q$: As we seen before h has coefficients in $k_0(\epsilon)$ and by definition has coefficients in E (is the irreducible polynomial of ϵ over E), then h has coefficients in Γ. $h(x)$ is irreducible in Γ (if not, h is not irreducible in E), consider the field extension $\Gamma' = \Gamma[x]/\langle h(x)\rangle$. As the roots of h are powers of ϵ and ϵ is a primitive root of the unity, then $k_0(\epsilon) \leq \Gamma'$. Γ' is a extension of degree q over Γ (because the degree of h is q), then $[k_0(\epsilon) : \Gamma]$ divides q ($k_0(\epsilon)$ is an intermediate extension between Γ and Γ'), as q is a prime number then $[k_0(\epsilon) : \Gamma]$ is equal to 1 or q , but $[k_0(\epsilon) : \Gamma]$ cannot be 1, because this implies that $k_0(\epsilon) = \Gamma$, this implies that $\epsilon \in E$, imposible. Then $[k_0(\epsilon) : \Gamma] = q$, as we want.

Let $\gamma = \epsilon^q$ and consider the field $k_0(\gamma)$, clearly $k_0(\gamma)$ is a subfield of the field $k_0(\epsilon)$.

(xii) The field $k_0(\gamma)$ contains all the q-roots of unity, since ϵ is a primitive q^{r+1}-root and therefore γ is a q^r-root of the unity. Clearly, we have that $k_0(\gamma)(\epsilon) = k_0(\epsilon)$. Since $\epsilon^q = \gamma$, then we have two cases $k_0(\epsilon) = k_0(\gamma)$ or $[k_0(\epsilon) : k_0(\gamma)] = q$. But the first case is impossible, indeed, $k_0(\epsilon) = k_0(\gamma) \subseteq k_0(\eta)$, this is a contradiction, since $\epsilon \in \overline{k} \setminus k_0(\eta)$. Therefore $[k_0(\epsilon) : k_0(\gamma)] = q$.

(xiii) The field $k_0(\epsilon)$ contains two different subfields, namely γ and $k_0(\eta)$. In fact this subfields are different because if $k_0(\eta) = \Gamma$, we have that $k_0(\eta) \subseteq E$ and therefore $\overline{k} = E(\eta) = E$, a contradiction with our hypothesis.

(xiv) $Gal(k_0(\eta)|k_0)$ is not cyclic: In a cyclic group there no exists two subgroups of the same order. Since $k_0(\epsilon)$ have two subfields of degree q, by Galois theory, we have that $Gal(k_0(\eta)|k_0)$ have two subgroups of order q.

To summarize, under the hypothesis that $Gal(\overline{k}|k_1) > 1$, we find a cyclotomic extension $k_0(\epsilon)$, with η a q^r-th root of unity, such that $Gal(k_0(\eta)|k_0)$ is not cyclic. By proposition 2.1.1 and proposition 2.1.2, this implies that $char(k_0) = 0$, $q = 2$ and $r = 2$ (the case when $r = 1$ is not possible, we see before that $r \geq 2$) and by (iii) we know that $[\overline{k} : E] = 2$. In

other words, we know that η is 4-th root of unity, but $i \in k_1 \subseteq E$ ($i = \sqrt{-1}$). Therefore the primitive 4-th root of unity i is an element of E, this implies that η is an element of E, this is a contradiction, contradicts that $E \subsetneq E(\eta) = \overline{k}$. Therefore is false to assume that $Gal(\overline{k}|k_1) > 1$ and therefore $Gal(\overline{k}|k_1) = 1$, equivalently $\overline{k} = k_1 = k(i)$, in other words, k is a real closed field. □

An equivalent formulation of the Artin-Schereier theorem (equivalent via Galois theory) says that there only two types of fields with a finite algebraic closure are algebraically closed fields and real closed fields.
Now, we want to restrict this discussion over algebraic extensions of the field of rational numbers. For this purposes we have to describe the relation between $\mathbb{Q}$, $\mathbb{R}^{alg}$ and $\overline{\mathbb{Q}}$.
The real closed fields can be characterized using order properties. In a real closed field, every element is either a square or the negative of a square. The set of non-zero square elements is a set of positive numbers, in other words, every real closed field is an ordered field. Furthermore, a real closed field is characterized as an ordered field such that its order can not be extended in any algebraic extension. The details of these facts are available in [Jacobson, 1964].

Definition 2.1.3. *Let k be an ordered field. An algebraic extension $L|k$ is called an **real closure** of k, if L is a real closed field and the order of L is an extension of the order of k.*

Every ordered field have a real closure and every two real closures of a field k are isomorphic. Similarly when we want to prove this properties for algebraic closure of a field, we use the Zorn lemma to guaranties the existence of real closures, by taking a maximal algebraic ordered extension (that extends the order) and we use extensions of order-isomorphisms, to guaranties the uniqueness under isomorphisms.
In particular, the real closure of the rational numbers $\mathbb{Q}$ is (under isomorphism) the field of the real algebraic numbers $\mathbb{R}^{alg}$, and the algebraic closure of the real algebraic numbers is (under isomorphism) the field of the algebraic numbers $\overline{\mathbb{Q}}$. This is the relation of these three fields and furthermore the Artin-Schreier theorem have a the next interpretation when we work in the category of algebraic extensions of $\mathbb{Q}$.

Theorem 2.1.2. *Let k be an algebraic extension of $\mathbb{Q}$. If Gal_k is finite, then either k is isomorphic to $\overline{\mathbb{Q}}$ or k is isomorphic to $\mathbb{R}^{alg}$*

Proof. If Gal_k is trivial, then k is algebraically closed and therefore k is isomorphic to $\overline{\mathbb{Q}}$.
If Gal_k is finite and no-trivial, then by the Artin-Schreier theorem k is real closed. In every closed field the element 1 is in the set of positive numbers (recall that in a real closed field every element is a square or the negative of an element is a square and the set of nonzero squares are the positive elements of the field, then there are only two possibilities either 1 is in the set of the positive elements or -1 is in the set of the positive numbers, but -1 cannot be, if -1 is in this set, then $1 = (-1)(-1)$ is an element of this set, a contradiction).Then

every positive integer is a positive element of k and therefore every rational number is a positive element of k. In other words, thus k is a real closed field that extends the order of $\mathbb{Q}$, k is a real closure of $\mathbb{Q}$. As we seen before, this implies that k is isomorphic to $\mathbb{R}^{alg}$ $\square$

In the category of the algebraic extensions of $\mathbb{Q}$, the condition of finiteness on the absolute Galois group is too restrictive and characterizes the isomorphy type of the fields with this property. In the next sections, this property is an example of an *anabelian* property.

2.2 Interlude in factorization of ideals

Definition 2.2.1. *Let k be a number field. The **ring of integers** of k is the integral closure of $\mathbb{Z}$, under the inclusion homomorphism $\mathbb{Z} \to k$. This ring is denoted by $\mathcal{O}_k$.*

Definition 2.2.2. *A domain A is called a **Dedekind domain**, if A is Noetherian, integrally closed and its krull dimension is one (equivalently, every non zero prime ideal is maximal).*

The Dedekind domains appeared naturally in algebraic number theory, the ring of integers of a number field is a Dedekind domain. One interesting properties about Dedekind domains is the unique factorization in the set of non-zero ideals (except in the order of the factors) as a products of distinct prime ideals.
Let k and l be number fields, such that l is an extension of k and P be a non-zero prime ideal of $\mathcal{O}_k$. By definition is clear that $\mathcal{O}_k \subseteq \mathcal{O}_l$, if we consider the extension of P in $\mathcal{O}_l$, $P\mathcal{O}_l$ this ideal maybe fails to be a prime ideal. However, $\mathcal{O}_l$ is a Dedekind domain, then there exists $n_1, ..., n_s$ positive integers and $P_1, ..., P_s$ distinct prime ideals of $\mathcal{O}_l$ such that,

$$P\mathcal{O}_l = P_1^{n_1} ... P_s^{n_s}.$$

Definition 2.2.3. *Let k, l and P as above. If $P\mathcal{O}_l$ is factorized in $\mathcal{O}_l$ as the product*

$$P\mathcal{O}_l = P_1^{n_1} ... P_s^{n_s},$$

*we say that a prime ideal Q of $\mathcal{O}_l$ is **lying over** P if $Q = P_i$, for some $i \in \{1, ..., s\}$, in other words, if Q appears in the factorization of $P\mathcal{O}_l$. This situation is denoted by $Q|P$.*

*The **ramification index** of a prime ideal Q lying over P is the exponent of Q that appears in the factorization, i.e., if $Q = P_i$ the ramification index of Q is n_i. This positive integer is denoted by $e(Q|P)$.*

If $Q|P$, then the next homomorphism of fields

$$\begin{aligned} \varphi : \mathcal{O}_k/P &\to \mathcal{O}_l/Q \\ x + P &\mapsto x + Q \end{aligned}$$

*is well defined, in other words, $\mathcal{O}_l/Q$ is field extension of $\mathcal{O}_k/P$. The **inertia degree** of $Q|P$, denoted by $f(Q|P)$, is the degree $[\mathcal{O}_l/Q : \mathcal{O}_k/P]$.*

In geometric language the situation as above, can be reinterpreted: if $\varphi : Spec(\mathcal{O}_l) \to Spec(\mathcal{O}_k)$ is the morphism of schemes induced by the inclusion map $\mathcal{O}_k \to \mathcal{O}_l$, then a point $Q \in Spec(\mathcal{O}_l)$ is above a point $P \in Spec(\mathcal{O}_k)$ if Q is an element of the fiber of P under φ, and the inertia degree is the degree of the extension of residual fields $k(Q)|k(P)$.
For Galois extension of number fields the rammification index and the inertial degree of a point does not change in elements of the same fiber. To be precise, we have the next theorem.

Theorem 2.2.1. *Let k and l be number fields, such that l is a (finite) Galois extension of k. If P is a non-zero prime ideal of $\mathcal{O}_k$, then for every two prime ideals of Q_1, Q_2 of $\mathcal{O}_l$ lying over P, we have that*

$$e(Q_1|P) = e(Q_2|P) \text{ and } f(Q_1|P) = f(Q_2|P).$$

The relation between the ramification index and the inertia degree is summarized in the next beautiful equation.

Theorem 2.2.2. *Let k be a number field and l a finite extension of k. If P is nonzero prime ideal of $\mathcal{O}_k$ and the factorization of P as a product of prime ideals in $\mathcal{O}_l$ is*

$$P\mathcal{O}_l = P_1^{n_1} ... P_s^{n_s},$$

then, if $n = [l : k]$, we have that

$$\sum_{i=1}^{s} e(P_i|P) f(P_i|P) = n.$$

In in addition, l is a Galois extension of k and $e = e(P_i|P)$, $f = f(P_i|P)$, for some $i \in \{1, ..., s\}$, then

$$sef = n.$$

Definition 2.2.4. *Let k be a number field and l a finite Galois extension of k. If P is a non-zero prime ideal of $\mathcal{O}_k$ and Q if prime of $\mathcal{O}_l$ lying over P, the **decomposition group** of Q over P, denoted by $D(Q|P)$, is defined by*

$$D(Q|P) := \{\sigma \in Gal(l|k) |\ \sigma(Q) = Q\},$$

*and the **inertia group** of $Q|P$, denoted by $I(Q|P)$, is defined by*

$$I(Q|P) = \{\sigma \in Gal(l|k) |\ \sigma(x) + Q = x + Q \text{ for all } x \in \mathcal{O}_l\}.$$

If k, l, P and Q are as in the above definition. The decomposition group and the inertia group of a ideal Q lying over P are subgroups of $Gal(l|k)$. Also, $I(Q|P)$ is a subgroup of $D(Q|P)$. Indeed, if $\sigma \in I(Q|P)$, then for all $x \in Q$, we have that

$$\sigma(x) + Q = x + Q = 0 + Q = Q,$$

thus, $\sigma(x) \in Q$, this proves that $\sigma(Q) \subseteq Q$. Reciprocally, if $x \in Q$, then as σ is an automorphism of L, then there exists $y \in L$, such that $\sigma(y) = x$, as x is integral over $\mathbb{Q}$, then the same is true for y, in other words, $y \in \mathcal{O}_l$. As $\sigma \in I(Q|P)$, we have that

$$y + Q = \sigma(y) + Q = x + Q = 0 + Q = Q,$$

therefore, $y \in Q$, then we have that $Q \subseteq \sigma(Q)$. This completes the proof of $I(Q|P) < D(Q|P)$.
In the same situation, define

$$\begin{aligned} F : D(Q|P) &\to Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P) \\ \sigma &\mapsto F(\sigma), \end{aligned}$$

here $F(\sigma)$ is the $\mathcal{O}_l/Q$-automorphism, defined by

$$\begin{aligned} F(\sigma) : \mathcal{O}_l/Q &\to \mathcal{O}_l/Q \\ x + Q &\mapsto \sigma(x) + Q, \end{aligned}$$

note that $F(\sigma)$ is well defined because $\sigma(Q) = Q$ and $F(\sigma)$ leave $\mathcal{O}_k/P$ fixes, because σ leave k fixes ($\mathcal{O}_k \subseteq k$). The kernel of F is the inertia group $I(Q|P)$. Indeed,

$$\begin{aligned} \sigma \in ker(F) &\Leftrightarrow F(\sigma) = id_{\mathcal{O}_l/Q}, \\ &\Leftrightarrow (\forall x \in \mathcal{O}_l/Q)(F(\sigma)(x) = id_{\mathcal{O}_l/Q}(x + Q)), \\ &\Leftrightarrow (\forall x \in \mathcal{O}_l/Q)(\sigma(x) + Q = x + Q), \\ &\Leftrightarrow \sigma \in I(Q|P). \end{aligned}$$

Then, we have the next exact sequence of groups,

$$1 \to I(Q|P) \to D(Q|P) \to Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P).$$

In particular, we know that $I(Q|P)$ is a normal subgroup of $D(Q|P)$ and by the first isomorphism theorem of groups, we obtain an injection

$$D(Q|P)/I(Q|P) \hookrightarrow Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P).$$

Let l and k be number fields, with l be a Galois extension of k. For every subgroup H of $Gal(l|k)$, we denote by l^H be the subfield of l fixed by the elements of H, concisely

$$l^H = \{x \in L | \sigma(x) = x \text{ for all } \sigma \in H\}.$$

For every subset X of l we denote by X^H the set $X \cap l^H$. For example $(\mathcal{O}_l)^H$ is equal to $\mathcal{O}_{l^H}$, the ring of integers of l^H. If Q is a prime ideal of $\mathcal{O}_l$, then Q^H is a prime ideal of $(\mathcal{O}_l)^H$. If Q is a non-zero prime ideal, then Q is a prime ideal lying over the non-zero prime ideal Q^H and moreover Q is the unique prime ideal lying over Q^H. Indeed, if Q_1 is a prime of $\mathcal{O}_l$ lying

over Q^H and $Q_1 \neq Q$, then $\mathcal{O}_l = Q_1 + Q$ (recall that, in a Dedekind domain every non-zero prime ideal is maximal). Therefore

$$\begin{aligned}(O_l)^H &= (Q_1 + Q) \cap l^H \\ &= Q_1 \cap l^H + Q \cap l^H \\ &= Q^H + Q^H \\ &= Q^H,\end{aligned}$$

a contradiction, thus Q is the unique ideal in $\mathcal{O}_l$ lying over Q^H. If P is a prime ideal of k and Q is a prime ideal of $\mathcal{O}_l$ lying over P then, under the canonical maps, $\mathcal{O}_l^H/Q^H$ is an intermediate extension between $\mathcal{O}_k/P$ and $\mathcal{O}_l/Q$.
Summarizing, let l be a finite Galois extension of a number field k. Every subgroup H of $Gal(l|k)$, produces the next objects

Group	Number field	Ring	Ideal	Residual field
H	l^H	$(\mathcal{O}_l)^H$	Q^H	$(\mathcal{O}_l)^H/Q^H$

Definition 2.2.5. *Let k be a number field and l be a finite Galois extension, P be a prime ideal of $\mathcal{O}_k$ and Q be a prime ideal of $\mathcal{O}_l$ lying over P. The* ***decomposition field*** *of $Q|P$, denoted by L_D is $l^{D(Q|P)}$, the subfield of l fixed pointwise by the elements of the decomposition group $D(Q|P)$. Similarly, the* ***inertia field*** *of $Q|P$ denoted by L_I, is the field $l^{I(Q|P)}$, fixed pointwise by the elements of the inertia group of $Q|P$.*

Theorem 2.2.3. *Let l be a finite Galois extension of a number field k, P be a prime ideal of $\mathcal{O}_k$ and Q be a prime ideal of $\mathcal{O}_l$ lying over P. If e is the ramification index of $Q|P$ and f is the inertia degree of $Q|P$, then*

(i) $[l : l_I] = e$.

(ii) l_I *is an extension of* l_D *and* $[l_E : l_D] = f$.

(iii) If $Q_I = Q^{I(P|Q)}$, *then* $e(Q|Q_I) = e$ *and* $f(Q|Q_I) = 1$.

(iv) If $Q_D = Q^{D(P|Q)}$, *then* Q_I *lies over* Q_D, $e(Q_I|Q_D) = 1$ *and* $f(Q_I|Q_D) = f$.

(v) The degree $[l : l_D]$ *is equal to the number of prime ideals in* $\mathcal{O}_l$ *lying over* P.

In some sense, the previous theorem states that if l is a finite Galois extension of a number field k, then for a prime ideal P of $\mathcal{O}_k$ the factorization of P in $\mathcal{O}_l$ occurs in levels. In the first level, associated to the decomposition field l_D, the ideal P is factorized in $\mathcal{O}_{l_I}$, as the product

$$P\mathcal{O}_{l_D} = Q_1 ... Q_s,$$

the ramification index and the inertia degree of any of this prime ideals in the decomposition is equal to 1. In the second level, associated to the inertia field, we obtain a factorization

$$P\mathcal{O}_{l_I} = P_1'...P_s',$$

we have the same number of prime ideals as in the first level, the difference between this factorization and the previous one is that, the inertia degree of the prime ideals in this factorization change and is equal to f, but the ramification index remains equal to 1. Finally, in $\mathcal{O}_l$ we obtain the factorization

$$P\mathcal{O}_{l_I} = P_1^e...P_s^e,$$

for some positive integer e, in other word, in this level the ramification appears, the inertia degree of any prime ideal in this factorization remains equal to f.

Corollary 2.2.1. *Let k be a number field and l be a Galois extension of k, P be a prime ideal of $\mathcal{O}_k$ and Q be a prime ideal of $\mathcal{O}_l$ lying over P. The sequence of groups and homomorphisms*

$$1 \to I(Q|P) \to D(Q|P) \to Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P) \to 1,$$

is exact.

Proof. The left exactness of this sequence has proved below. Only we need to prove the surjectivity of the homomorphism

$$\begin{aligned} F : D(Q|P) &\to Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P) \\ \sigma &\mapsto F(\sigma) \end{aligned}$$

this is equivalent to prove that the canonical group injection induced in the quotient $D(Q|P)/I(Q|P) \hookrightarrow Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P)$ is an isomorphism. . Then, using Galois theory and the part (ii) of the previous theorem we have

$$\begin{aligned} D(Q|P)/I(Q|P) &= [l_I : l_D] \\ &= [\mathcal{O}_l/Q : \mathcal{O}_k/P] \\ &= Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P) \end{aligned}$$

therefore, $D(Q|P)/I(Q|P) \hookrightarrow Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P)$ is an isomorphism.

□

2.3 Chebotarev's density theorem and its consequences

In order to understand the characterization via Galois groups of the number fields, we study consequences of the Chebotarev density theorem, we not focus our attention in the proof, which involves class field theory and other methods not discussed here, instead, we study the consequences of this theorem, in particular, the characterization of Galois extensions in terms of prime ideals that split completely.

Definition 2.3.1. *Let l be a finite extension of a number field k and let P be prime ideal of $\mathcal{O}_k$*

*(i) We say that P **splits completely** in L, if for every prime ideal Q of $\mathcal{O}_l$ lying over P we have that $e(Q|P) = f(Q|P) = 1$.*

*(ii) We say that P **have a factor of degree one** in if there exists a prime ideal Q of $\mathcal{O}_l$ lying over P such that $f(Q|P) = 1$.*

*(iii) We say that P is **unramified** in L if for every prime ideal Q of $\mathcal{O}_l$ lying over P we have that $e(Q|P) = 1$.*

We denote by $Spl(l|k)$ the set of prime ideals of $\mathcal{O}_K$ that split completely in L and by $Spl_1(l|k)$ the set prime ideals of $\mathcal{O}_k$ unramified in L with a factor of degree one.

Suppose that l is a Galois extension of k and $e(Q|P) = 1$. Theorem 2.2.3 implies that l is equal to the inertia field of $Q|P$. Therefore, Galois theory implies that

$$\begin{aligned} I(Q|P) &= Gal(L|L_I) \\ &= Gal(L|L) \\ &= \{1\}. \end{aligned}$$

Since $I(Q|P)$ is the kernel of the surjective homomorphism

$$\begin{aligned} F : D(Q|P) &\to Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P) \\ \sigma &\mapsto F(\sigma) \end{aligned}$$

where $F(\sigma)(x+Q) = \sigma(x)+Q$. Therefore F is an ismorphism. Since $\mathcal{O}_l/Q|\mathcal{O}_k/P$ is a finite extension of finite fields, then $Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P)$ is cyclic, generated by the frobenius automorphism. Therefore, we can find a unique element $Frob_P^Q \in D(Q|P)$ such that $F(Frob_P^Q)$ is the Frobenius automorphism of $\mathcal{O}_l/Q|\mathcal{O}_k/P$.

Definition 2.3.2. *Let l be a finite Galois extension of a number field k, P be a prime ideal of $\mathcal{O}_k$, Q be a prime ideal of $\mathcal{O}_l$ such that Q lying over P and $e(Q|P) = 1$. The **frobenius element** of $Q|P$, denoted by $Frob_P^Q$, is the unique element of $D(Q|P)$, such that $Frob_P^Q(x) + Q = x^q + Q$, where $q = |\mathcal{O}_k/P|$.*

Let l be a finite extension of a number field k, P be a prime ideal of $\mathcal{O}_k$ and $\mathcal{P}$ be the set of prime ideals of $\mathcal{O}_l$ lying over P, define the action

$$\begin{aligned} . : Aut(l|k) \times \mathcal{P} &\to \mathcal{P} \\ (\sigma, Q) &\mapsto \sigma(Q) \end{aligned}$$

If $Q \in \mathcal{P}$, then the stabilizer of Q is precisely the decomposition group $D(Q|P)$. If $\sigma \in Gal(l|k)$, then

$$D(\sigma(Q)|P) = \sigma D(Q|P)\sigma^{-1},$$

in other words, if two elements of $\mathcal{P}$ are in the same orbit, then their decomposition groups are $Aut(l|k)$-conjugates.
If in addition l is a Galois extension of k, then this action is transitive (in particular all the decomposition groups of elements of $\mathcal{P}$ are $Gal(l|k)$-conjugates). Assume that P is unramified, therefore for every $Q \in \mathcal{P}$, $Frob_P^Q$ is defined, and we have that $\sigma^{-1} \circ Frob_P^Q \circ \sigma = Frob_P^{\sigma(Q)}$. Indeed, if $q = |\mathcal{O}_k/P|$, then

$$\begin{aligned} F(\sigma^{-1} \circ Frob_P^Q \circ \sigma)(x) &= \sigma^{-1} \circ Frob_P^Q \circ \sigma(x) + \sigma(Q) \\ &= \sigma^{-1}(Frob_P^Q(\sigma(x))) + \sigma(Q) \\ &= \sigma^{-1}((\sigma(x))^q) + \sigma(Q) \\ &= (\sigma^{-1}(\sigma(x)) + \sigma(Q) \\ &= x^q + \sigma(Q). \end{aligned}$$

Thus, under the hypothesis of that P is unramified, for every $Q \in \mathcal{P}$, we have that

$$\begin{aligned} C_Q &= \{\sigma^{-1} \circ Frob_P^Q \circ \sigma | \sigma \in Gal(l|k)\} \\ &= \{Frob_P^R | R \in \mathcal{P}\}. \end{aligned}$$

In other words, the conjugancy class C_Q of Q consist of the frobenius elements associated to the elements of $\mathcal{P}$.

Definition 2.3.3. *Let l be a finite Galois extension of a number field k and P be a prime ideal of $\mathcal{O}_k$ unramified in l. The **frobenius element** of P in l is the conjugancy class (as below) C_Q for some (and thus for all) $Q \in \mathcal{P}$, this is class by $Frob_P^l$.*

Let I be a non-zero ideal of $\mathcal{O}_k$. The **absolute norm** of I, denoted by $\mathfrak{N}(I)$, is the natural number $|\mathcal{O}_k/I|$. Let S be a set of nonzero prime ideals of $\mathcal{O}_k$.

(i) The **natural density** of S is defined by

$$\delta(S) = \lim_{N\to\infty} \frac{|\{P \in S | \mathfrak{N}(P) \leq N\}|}{|\{P \in Spec(\mathcal{O}_k) \setminus \{0\} | \mathfrak{N}(P) \leq N\}|},$$

if this limit exists.

(ii) The **Dirichlet density** of S is defined by

$$d(S) = \lim_{s\to 1^+} \frac{\sum_{P\in S} \frac{1}{\mathfrak{N}(p)^s}}{\sum_{P\in Spec(\mathcal{O}_k)\setminus\{0\}} \frac{1}{\mathfrak{N}(p)^s}}$$

if this limit exists

If the natural density exists, then the Dirichlet density exists and they are equal.
Let l be a finite Galois extension of a number field k. Denote by U_k^l the set of primes of k unramified in l. For every $\sigma \in Gal(l|k)$, let

$$P_{l|k}(\sigma) = \{P \in U_k^l | \text{ exists a prime ideal } Q \text{ of } \mathcal{O}_l \text{ such that, } \sigma = Frob_P^Q\},$$

Chebotarev's density theorem says how to compute the density of the set $P_{l|k}(\sigma)$, for every $\sigma \in Gal(l|k)$.

Theorem 2.3.1. ***(Chebotarev density theorem)***
Let l be finite Galois extension of a number field k. For every $\sigma \in Gal(l|k)$, the Dirichlet density of $P_{l|k}(\sigma)$ exists and moreover,

$$d_{l|k}(\sigma) = \frac{|\langle\sigma\rangle|}{|Gal(l|k)|}$$

where $\langle\sigma\rangle$ is the conjugancy class of σ.

Let k be a number field, S and T two sets of prime ideals of k. We denote by $S\hat{\subseteq}T$ if there exists S_0 a finite subset of S such that $S \setminus S_0 \subseteq T$, and by $S\hat{=}T$ if $S\hat{\subseteq}T$ and $T\hat{\subseteq}S$. For example, if l is a finite extension of k and N is a finite Galois extension of k containing l, then

$$Spl_1(l|k)\hat{=}\bigsqcup_{\sigma\in H} P_{N|k}(\sigma)$$

where

$$H = \{\sigma \in Gal(N|k) | \langle\sigma\rangle \cap Gal(N|l) \neq \emptyset\}.$$

Proposition 2.3.1. *If l is a finite extension of a number field k, then*

$$d(Spl_1(l|k)) \geq \frac{1}{[l:k]}.$$

Moreover, we have that,

$$d(Spl_1(l|k)) = \frac{1}{[l:k]} \text{ if and only if } l \text{ is a Galois extension of } k.$$

Proof. Let N be a finite Galois extension of k containing l (for example the Galois closure of $l|k$), then

$$Spl_1(l|k)\hat{=}\bigsqcup_{\sigma\in H} P_{N|k}(\sigma)$$

where

$$H = \{\sigma \in Gal(N|k) | \langle\sigma\rangle \cap Gal(N|l) \neq \emptyset\}.$$

Therefore

$$\begin{aligned} d(Spl_1(l|k)) &= d(\bigsqcup_{\sigma\in H} P_{N|k}(\sigma)) \\ &= \sum_{\sigma\in H} d(P_{N|k}(\sigma)) \\ &= \sum_{\sigma\in H} \frac{|\langle\sigma\rangle|}{|Gal(N|k)|} \\ &= \frac{1}{|Gal(N|k)|}\sum_{\sigma\in H} |\langle\sigma\rangle| \\ &= \frac{1}{|Gal(N|k)|}|\bigsqcup_{\sigma\in H}\langle\sigma\rangle|. \end{aligned}$$

If $\sigma \in Gal(N|l)$, then $\sigma \cap Gal(N|l) \neq \emptyset$. In other words, $\sigma \in H$, this implies that

$$Gal(N|l) \subseteq \bigsqcup_{\sigma\in H}\langle\sigma\rangle,$$

and therefore,

$$|Gal(N|l)| \leq |\bigsqcup_{\sigma\in H}\langle\sigma\rangle|,$$

Thus,

$$\begin{aligned} d(Spl_1(l|k) &\geq \frac{|Gal(N|l)|}{|Gal(N|k)|} \\ &= \frac{1}{\frac{|Gal(N|l)|}{|Gal(N|k)|}} \\ &= \frac{1}{(Gal(N|k) : Gal(N|l)} \\ &= \frac{1}{[k:l]} \end{aligned}$$

This proves the first part, the second part is deduced from Galois theory. Indeed,

$$\begin{aligned} l|k \ is \ Galois &\Leftrightarrow Gal(N|L) \ is \ a \ normal \ subgroup \ of \ Gal(N|k) \\ &\Leftrightarrow (\forall_{\sigma\in Gal(N|k)})(\langle\sigma\rangle \cap Gal(N|l) \neq \emptyset \Rightarrow \sigma \subseteq Gal(N|l)) \\ &\Leftrightarrow Gal(N|L) = \bigsqcup_{\sigma\in H}\langle\sigma\rangle \\ &\Leftrightarrow d(Spl_1(l|k)) = \frac{1}{n}, \end{aligned}$$

the last equivalence is a consequence of the finiteness of $Gal(N|l)$. □

Recall that if l and $l^{'}$ are finite extension of a number field k, then a prime ideal P of $\mathcal{O}_k$ splits completely in $l \vee l^{'}$ (the composition of l and $l^{'}$) if, and only if P splits completely in l and $l^{'}$. This implies that if l if a finite extension of a number field k and N is the Galois closure of $l|k$, then a prime ideal of k splits completely in l if and only if splits completely in N (N is a finite composition of finite extensions of l).

Proposition 2.3.2. *Let l be a finite extension of a number field k. If almost all prime ideal of $\mathcal{O}_k$ splits completely (except for a finite set), then $l = k$.*

Proof. Notice that the Dirichlet density of a finite set of primes is 0. Therefore, $d(Spl(l|k)) = d(Spec(\mathcal{O}_k \backslash \{0\}) = 1$, by hypothesis. Let N be the Galois closure of $l|k$, therefore $Spl(N|k) = Spl(l|k)$, and we have that

$$\begin{aligned} 1 &= d(Spl(l|k) \\ &= d(Spl(N|k) \\ &= \frac{1}{[N:k]} \end{aligned}$$

therefore $[N : k] = 1$. In other words, $N = l = k$. □

Corollary 2.3.1. *Let l be a finite extension of k. l is Galois if and only if $Spl_1(l|k) = Spl(l|k)$.*

Proof. If $l|k$ is Galois then theorem 2.2.1 implies that $Spl_1(l|k) = Spl(l|k)$.

Assume that $Spl_1(l|k) = Spl(l|k)$, let N be the Galois closure of $l|k$. Then,

$$\begin{aligned} Spl_1(l|k) &= Spl(l|k) \\ &= Spl(N|k) \\ &= Spl_1(N|K), \end{aligned}$$

therefore $d(Spl_1(l|k)) = d(Spl_1(N|k))$, thus

$$\begin{aligned} \frac{1}{[N:k]} &= d(Spl_1(N|k)) \\ &= d(Spl_1(L|k)) \\ &\geq \frac{1}{[l:k]}, \end{aligned}$$

therefore $[l : k] = [N : k]$, in other words $l = N$, in other words, l is a Galois extension of k. □

Surprisingly the Chebotarev's density theorem has a strong implication namely the Brauer theorem which characterized the finite Galois extensions over a number field in terms of the set of primes that splits completely. To be precise.

Theorem 2.3.2. ***(Brauer)*** *Let l be a Galois extension of a number field k and M be a finite extension of k.*

$$L \subseteq M \text{ if, and only if } Spl_1(M) \subseteq Spl_1(l).$$

Proof. Suppose that $L \subseteq M$. If $P \in Spl_1(M)$ there exists a prime ideal Q of $\mathcal{O}_M$ lying over P, such that $e(Q|P) = f(Q|P) = 1$. The prime ideal $Q_1 = Q \cap \mathcal{O}_l$ of $\mathcal{O}_l$ lies over P and $e(Q_1|P)$, $f(Q_1|P)$ divides $e(Q|P)$ and $f(Q|P)$, respectively. Therefore, $e(Q_1|P) = f(Q_1|P) = 1$ and this implies that $P \in Spl_1(l)$.

Suppose that $Spl_1(M) \subseteq Spl_1(l)$. Let N be a finite Galois extension of k containing M and l (for example the Galois closure of $M \vee l|k$). Let

$$H = \{\sigma \in Gal(N|k) | \, \langle\sigma\rangle \cap Gal(N|M) \neq \emptyset\},$$

and

$$H' = \{\sigma \in Gal(N|k) | \, \langle\sigma\rangle \cap Gal(N|l) \neq \emptyset\}.$$

By assumption we have that

$$\begin{aligned} \bigsqcup_{\sigma \in H} P_{N|k}(\sigma) &\hat{=} Spl_1(M|k) \\ &\subseteq Spl_1(L|k) \\ &\hat{=} \bigsqcup_{\sigma \in H'} P_{N|k}(\sigma) \end{aligned}$$

Let $\sigma \in Gal(N|M)$ and consider the set of primes $P_{N|k}(\sigma)$, this set of primes have finite Dirichlet density, then it is infinite and in particular a non-empty set, let $P \in P_{N|k}(\sigma)$, then $P \in \bigsqcup_{\sigma \in H} P_{N|k}(\sigma)$ and therefore $P \in \bigsqcup_{\sigma \in H'} P_{N|k}(\sigma)$, i.e., there exists a unique $\tau \in H'$, such that $P \in P_{N|k}(\tau)$. In particular, $P \in P_{N|k}(\tau) \cap P_{M|k}$, which implies that $\langle\sigma\rangle$ and $\langle\tau\rangle$ are the frobenius element of P, therefore $\langle\sigma\rangle = \langle\tau\rangle$, but $\langle\tau\rangle \cap Gal(N|l) \neq \emptyset$ and $Gal(N|l)$ is a normal subgroup of $Gal(N|k)$ (l is a Galois extension of k), therefore $\sigma \in Gal(N|l)$. We just prove that $Gal(N|M) \subseteq Gal(N|l)$, by Galois theory we have that $l \subseteq M$. □

Corollary 2.3.2. *Let l and l' be two finite Galois extension of a number field k.*

$$l = l' \text{ if, and only if } Spl(l|k) = Spl(l'|k).$$

2.4 Neukirch theorems

In this section we study the characterization of some closed subgroups of the absolute Galois group of the rational numbers $Gal_{\mathbb{Q}}$.

By Galois theory every closed subgroup H of $Gal_{\mathbb{Q}}$, is equal to $Gal(\overline{\mathbb{Q}}|k)$ for some subfield k of $\overline{\mathbb{Q}}$, in particular, k is algebraic over $\mathbb{Q}$, then we can identify $\overline{k}$ with $\overline{\mathbb{Q}}$. We have that $H = Gal(\overline{\mathbb{Q}}|k) = Gal(\overline{k}|k) = Gal_k$. In other words, the closed subgroups of $Gal_{\mathbb{Q}}$ are absolute Galois groups of some algebraic extension of $\mathbb{Q}$.
First, we characterizes the finite subgroups of $Gal_{\mathbb{Q}}$. The trivial subgroup of $Gal_{\mathbb{Q}}$ is equal to the absolute Galois group $Gal_{\overline{\mathbb{Q}}}$. If H is a finite and non-trivial subgroup of $Gal_{\mathbb{Q}}$, in particular, H is closed ($Gal_{\mathbb{Q}}$ have profinite topology) then H is equal to Gal_k, for some subfield k of $\overline{\mathbb{Q}}$, therefore theorem 2.1.2 implies that k is isomorphic to $\mathbb{R}^{alg}$, without lose of generality lets suppose that $\mathbb{R}^{alg}$ is a subfield of $\overline{\mathbb{Q}}$. Let $\varphi : k \to \mathbb{R}^{alg}$ be an isomorphism, clearly this isomorphism is a $\mathbb{Q}$-isomorphism. We can extend φ to an automorphism $\hat{\varphi} : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$, $\hat{\varphi}$ produces an conjugation-isomorphism between the absolute Galois groups of k and $\mathbb{R}^{alg}$. Concisely,

$$\begin{aligned} \hat{\varphi} : Gal_k &\to Gal_{\mathbb{R}^{alg}} \\ \sigma &\mapsto \hat{\varphi} \circ \sigma \circ \hat{\varphi}^{-1} \end{aligned}$$

is an isomorphism, we just prove the following.

Theorem 2.4.1. ***(Characterization of finite subgroups of*** $Gal_{\mathbb{Q}}$ ***)***
Let H be a finite subgroup of $Gal_{\mathbb{Q}}$. We have the next two possibilities

(i) H is trivial, in this case $H = Gal_{\overline{\mathbb{Q}}}$. Or,

(ii) H has order two, in this case there exists a subfield k of $\mathbb{Q}$ and an element $\hat{\varphi} \in Gal_{\mathbb{Q}}$, such that $H = Gal_k$, $\hat{\varphi}$ restricted to k is an isomorphism with $\mathbb{R}^{alg}$ and

$$\begin{aligned} \psi : Gal_k &\to Gal_{\mathbb{R}^{alg}} \\ \sigma &\mapsto \hat{\varphi} \circ \sigma \circ \hat{\varphi}^{-1} \end{aligned}$$

is a group isomorphism.

In order to characterize another closed subgroups of $Gal_{\mathbb{Q}}$, recall that the field of real numbers $\mathbb{R}$ is only one of the completions of the rational number $\mathbb{Q}$, the completion with respect to the euclidean norm. We obtain a similar result if we repeat this process with all the completions of $\mathbb{Q}$? This is the question behind the Neukirch's results. Let p a prime number, choose an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ embedded in an algebraic closure of $\mathbb{Q}_p$. The field of *algebraic p-adic numbers* $\mathbb{Q}_p^{alg}$, is the field $\overline{\mathbb{Q}} \cap \mathbb{Q}_p$ (this intersection is taken in $\overline{\mathbb{Q}_p}$). The idea of Neukirch is try to characterize the albebraic fields k over $\mathbb{Q}$, such that $Gal_k \simeq Gal_{\mathbb{Q}_p^{alg}}$.

Theorem 2.4.2. ***(Neukirch's theorem)*** *Let k be a number field, l be a p-adic field (a finite extension of $\mathbb{Q}_p$. If Gal_k has a closed subgroup H isomorphic to Gal_l, then there exists a prime P of k lying over $\langle p \rangle$, and a prime Q of k^{sep} lying over P, such that $H \subseteq D(Q|P)$, and $[l : \mathbb{Q}_p] \geq [k_P : \mathbb{Q}_p]$.*

Recall that, the non-zero primes of the ring of integers of a number field are in correspondence with finite places of the number field. The primes in a infinite field extension are finite places, and the relation of lye over is the relation of extend in the sense of valuations.
The proof of Neukirch's theorem involves cohomology of number fields and other techniques not discussed here. Instead, we discuss some consequences of this theorem. For details about the proof see **??**.

Corollary 2.4.1. *Let k be a number field, p be a prime number and P be a prime ideal of $\mathcal{O}_k$ lying over $\langle p\rangle$. A subgroup of Gal_k is the decomposition subgroup of some prime lying over P if and only it is maximal with respect to the closed subgroups of Gal_k isomorphic to Gal_l, for some p-adic field l.*

Let k_1 and k_2 be two number fields and

$$\sigma : Gal_{k_1} \to Gal_{k_2}$$

be a continuous isomorphism. Let P be a prime of k_1 and Q be a prime of k_1^{sep} lying over P. Consider the decomposition group $D(Q|P)$, then $\sigma(D(Q|P))$ is a subgroup of Gal_{k_2}, and moreover σ restricts to an isomorphism between $D(Q|P)$ and $\sigma(D(Q|P))$, by the previous corollary we know that the closed subgroup $D(Q|P)$ of Gal_{k_1} is isomorphic to Gal_l for some p-adic field l (p is the prime number generating the ideal $P \cap \mathbb{Z}$) and $D(Q|P)$ is maximal in the closed groups of Gal_{k_1} with this property, then the same is true for the subgroup $\sigma(D(Q|P))$, therefore by the previous corollary, there exists a prime $P^{'}$ of k_1, a prime $Q^{'}$ of k^{sep} lying over $P^{'}$, such that $\sigma(D(Q|P)) = D(Q^{'}|P^{'})$, thus σ induces a function between the primes of k_2^{sep} and the primes of k_1^{sep}. Before we study the behavior of this function first we introduce some definitions.
For every number field l be denote by D the set of prime ideals of l, associate to D_l the discrete topology, then D_l is a locally compact Hausdorff space and denote by $Sp(l)$ be the Alexandroff compactification (by one point). In other words, $Sp(l)$ is the topological space $Spec(\mathcal{O}_l)$, the point at infinity added in the Alexandroff compactification corresponds to the generic point of $Spec(\mathcal{O}_l)$.
If k_1 and k_2 are two number fields and $k_1 \leq k_2$, we have a projection $\pi_{k_1,k_2} : Sp(k_2) \to Sp(k_1)$; $P \mapsto P \cap k_1$. In particular every number field have canonical projection $\pi_{k_1,\mathbb{Q}}$, denoted by π_{k_1}. If k is a infinite extension of $\mathbb{Q}$, $Sp(l)$ is the projective limit space of the directed system

$$\{(Sp(l), \pi_{l,l'|l,l'} \text{ are number field and } l^{'}l \leq k\}.$$

Recall that the projective limit of compact and Hausdorff spaces is compact and Hausdorff too. Moreover, $Sp(k)$ is a profinite space, in other words, $Sp(k)$ is, in addition, totally disconnected. As a set $Sp(k)$ is the set of primes of k with a point added and is a generic point for $Sp(k)$.
Denote by η_1 and η_2 be the generic points of $Sp(k_1)$ and $Sp(k_2)$, respectively. Using this language, we know that every continuous isomorphism

$$\sigma : Gal_{k_1} \to Gal_{k_2}$$

induces a correspondence between the primes of k_2 and the primes of k_2, if we added to this correspondence the generic points, then σ induces the correspondence

$$\begin{array}{rcl} Sp(\sigma) : Sp(k_1^{sep}) & \to & Sp(k_2^{sep}) \\ P & \mapsto & \begin{cases} Q \quad if \quad \sigma(D(P|P \cap k_1)) = D(Q|Q \cap k_2) \\ \\ \eta_1 \quad if \qquad\qquad\qquad P = \eta_1 \end{cases} \end{array}$$

On the other hand, let

$$H_1 = \{l_1 \leq k_1^{sep} | l_1 \text{ is an extension of } k_1\}, \text{ and}$$

$$H_2 = \{l_2 \leq k_2^{sep} | l_2 \text{ is an extension of } k_2\}.$$

By Galois theory, we know that H_1 and the closed subgroups of Gal_{k_1} are in correspondence, via the function $H_1 \to CS(Gal_{k_1})$; $l_1 \mapsto Gal(k_1^{sep}|l_1)$. Similarly we have a correspondence between H_2 and Gal_{k_2}. Since σ induces a correspondence between closed subgroups of Gal_{k_2} and closed subgroups of Gal_{k_1}, then σ induces a correspondence between H_1 and H_2, concretely

$$\begin{array}{rcl} \hat{\sigma} : H_2 & \to & H_1 \\ l_2 & \mapsto & l_1 \ \ if \ \ \sigma(Gal(k_2^{sep}|l_2)) = Gal(k_1^{sep}|l_1) \end{array}$$

Using this correspondence and once again corollary 2.4.1, we have that for every $l_2 \in H_2$, we have a correspondence

$$Sp(\sigma)_{l_2} : Sp(l_2) \to Sp(\hat{\sigma}(l_2))$$

Theorem 2.4.3. ***(Finite local correspondence)*** *Let k_1 and k_2 be two number fields. If $\sigma : Gal_{k_2} \to Gal_{k_1}$ is an isomorphism, then for every finite extension l_2 of k_2, with $l_2 \in H_2$, we have that $Sp(\sigma)_{l_2}$ is an homeomorphism.*

Proof. l_2 and $\hat{\sigma}(l_2)$ are finite number fields, then $Sp(l_2)$ and $Sp(\hat{\sigma}(l_2))$ are Alexandroff compactification of discrete spaces, therefore $Sp(\sigma)_{l_2}$ is trivially an homeomorphism if we restrict to such discrete subspaces. Since $Sp(\sigma)_{l_2}$ send the generic point of $Sp(l_2)$ to the generic point of $Sp(\hat{l_2})$, then the theorem holds. □

We omit the proof of the next proposition, which involves techniques of cohomology of number fields, for details of the proof see [37].

Proposition 2.4.1. *If k_1 and k_2 are two number fields. If $\sigma : Gal_{k_1} \to Gal_{k_2}$, for every finite extension l_2 of k_2, then the next diagram is commutative*

$$\begin{array}{ccc} Sp(l_2) & \xrightarrow{Sp(\sigma)_{l_2}} & Sp(\hat{\sigma}(l_2)) \\ & {\scriptstyle \pi_{l_2}} \searrow \quad \swarrow {\scriptstyle \pi_{\sigma(\hat{l}_2)}} & \\ & Sp(\mathbb{Q}) & \end{array}$$

Theorem 2.4.4. ***(Local correspondence)*** *Let k_1 and k_2 be two number fields. If $\varphi : Gal_{k_1} \to Gal_{k_2}$ is an isomorphism of profinite groups, then for every extension l_2 of k_2,*

$$Sp(\sigma)_{l_2} : Sp(l_2) \to Sp(\hat{\sigma})$$

is an homeomorphism.

Proof. $Sp(\sigma)_{l_2}$ is the inverse limit of $\{Sp(\sigma)_{l_2'}\}_{l_2' \in \Gamma}$, where

$$\Gamma = \{l_2' \leq l_2 | l_2' \text{ is a finite extension of } k_2\}.$$

By the previous proposition we know that $Sp(\sigma)_{l_2}$ commutes with the projection, this and the finite local correspondence implies the result. □

2.5 Galois characterization of number fields.

In this section for every field k, fix an algebraic closure $\overline{k}$ and we denote by k^{sep} the separable closure of k inside $\overline{k}$.
Let k_1 and k_2 be two fields denote by $Iso(k_1^{sep}|k_1, k_2^{sep}|k_2)$ the set of isomorphisms $\varphi : k_1^{sep} \to k_2^{sep}$ such that $\varphi(k_1) = k_2$. $\varphi \in Iso(k_1^{sep}|k_2, k_2^{sep}|k_2)$, induces an isomorphism of profinite groups (with inverse $((\varphi^{-1})^*)$

$$\begin{array}{rcl} \varphi^* : Gal_{k_2} & \to & Gal_{k_1} \\ \sigma & \mapsto & \varphi \circ \sigma \circ \varphi^{-1}. \end{array}$$

If G and H are profinite groups, denote by $Iso(G, H)$ be the set of continuous isomorphisms from G to H and by $Aut(G) = Iso(G, G)$. We can define a function

$$\begin{array}{rcl} * : Iso(k_1^{sep}|k_2, k_2^{sep}|k_2) & \to & Iso(Gal(k_2^{sep}|k_2), Gal(k_1^{sep}|k_1)) \\ \varphi & \mapsto & \varphi^*, \end{array}$$

In this section we study the behavior of this function. Starting with two consequences of Krasner's lemma.

Proposition 2.5.1. *Let k be a number field. If P and Q are two different primes of k^{sep}, then $D(P|P \cap \mathbb{Q}) \cap D(Q|Q \cap \mathbb{Q}) = 1$.*

Proposition 2.5.2. *If k_1 is a Galois finite extension of k_2, then the homomorphism*

$$\begin{aligned} F : Gal_{k_2} &\to Aut(Gal_{k_1}) \\ \sigma &\mapsto F_\sigma \end{aligned}$$

is inyective. where,

$$\begin{aligned} F_\sigma : Gal_{k_1} &\to Gal_{k_1} \\ \theta &\mapsto \sigma \circ \theta \circ \sigma^{-1}. \end{aligned}$$

Proof. Without losing generality, suppose that $k_1^{sep} = k_2^{sep}$. Since $k_2 \leq k_1$, then $Gal_{k_1} \subseteq Gal_{k_2}$, then F_σ make sense for every $\sigma \in Gal_{k_2}$. Let σ be elements of Gal_{k_2} such that $F_{\sigma_1} = id_{Gal_{k_1}}$, then for every prime P of k_2^{sep}, we have that

$$F_\sigma(D(P|P \cap k_2) \cap Gal_{k_1})) = D(P|P \cap k_2) \cap Gal_{k_1}.$$

But $F_\sigma(D(P|P \cap k_2) \cap Gal_{k_1})) = D(\sigma(P)|\sigma(P) \cap k_2) \cap Gal_{k_1}$:

($\subseteq$) If $\theta \in D(P|P \cap k_2) \cap Gal_{k_1}$, then $\theta(P) = P$ and therefore

$$\begin{aligned} F_\sigma(\theta)(\sigma(P)) &= \sigma \circ \theta \circ \sigma^{-1}(\sigma(P)) \\ &= \sigma \circ \theta(P) \\ &= \sigma(P). \end{aligned}$$

($\supseteq$) If $\theta \in D(\sigma(P)|\sigma(P) \cap k_2) \cap Gal_{k_1}$, we have that $\theta(\sigma(P)) = \sigma(P)$. Let $\theta_1 = \sigma^{-1} \circ \theta \circ \sigma$, then $F_\sigma(\theta_1) = \theta$ and

$$\begin{aligned} \theta_1(P) &= \sigma^{-1} \circ \theta \circ \sigma(P) \\ &= \sigma^{-1}(\theta(\sigma(P)) \\ &= \sigma^{-1}(\sigma(P)) \\ &= P. \end{aligned}$$

Thus, $D(P|P \cap k_2) \cap Gal_{k_1} = D(\sigma(P)|\sigma(P) \cap k_2) \cap Gal_{k_1}$. Therefore,

$$\begin{aligned} 1 &\neq D(P|P \cap k_2) \cap Gal_{k_1} \\ &= D(P|P \cap k_2) \cap D(\sigma(P)|\sigma(P) \cap k_2) \cap Gal_{k_1} \\ &\subseteq D(P|P \cap k_2) \cap D(\sigma(P)|\sigma(P) \cap k_2) \end{aligned}$$

implies that $P = \sigma(P)$ for every prime P of k_2^{sep}. Take two different primes P and Q of k_2^{sep}, then $\sigma = 1$, since $\sigma \in D(P|P \cap k_2) \cap D(Q|Q \cap k_2) = \{1\}$. □

Corollary 2.5.1. *If k_1 and k_2 are two number fields then the function*

$$\begin{array}{rcl} * : Iso(k_1^{sep}|k_2, k_2^{sep}|k_2) & \to & Iso(Gal(k_2^{sep}|k_2), Gal(k_1^{sep}|k_1)) \\ \varphi & \mapsto & \varphi^*, \end{array}$$

is injective.

Proof. Let N be the Galois closure of $k_1 \vee k_2$ over $\mathbb{Q}$, without losing generality, suppose that $N^{sep} = k_1^{sep} = k_2^{sep} = \overline{\mathbb{Q}}$. Let $\varphi_1, \varphi_2 \in Iso(k_2^{sep}|k_2, k_1^{sep}|k_1)$, such that $\varphi_1^* = \varphi_2^*$, in particular we have that

$$\varphi_1^*|_{Gal(k_1^{sep}|N)} = \varphi_2^*|_{Gal(k_1^{sep}|N)},$$

Consider the homomorphism

$$F : Gal_{\mathbb{Q}} \to Aut(Gal_N)$$

as we defined in the previous proposition. Then, $F_{\varphi_1} = F_{\varphi_2}$, indeed if $\sigma \in Gal_N$, then

$$\begin{array}{rcl} F_{\varphi_1}(\sigma) & = & \varphi_1 \circ \sigma \circ \varphi_1^{-1} \\ & = & \varphi_1^*(\sigma) \\ & = & \varphi_1^*|_{(\sigma)} \\ & = & \varphi_2^*|_{Gal_N}(\sigma) \\ & = & \varphi_2 \circ \sigma \circ \varphi_2^{-1} \\ & = & F_{\varphi_2}(\sigma) \end{array}$$

therefore, $\varphi_1 = \varphi_2$. □

Corollary 2.5.2. *If k is a number field, then Gal_k has trivial center.*

Proof. If σ is an element in the center of Gal_k, then σ is in the kernel of the homomorphism $F : Gal_k \to Aut(Gal_k)$ and thus $\sigma = 1$. □

In order to understand the next theorem we make some remarks first. Let $\sigma \in Iso(Gal_{k_1}, Gal_{k_2})$, then we know that σ induces a function between the algebraic extensions of k_1 and the algebraic extensions of k_2, this correspondence is denoted by $\hat{\sigma}$, as in the previous section. For every algebraic extension l_1 of k_1, σ induces an homeomorphism $Sp(\sigma)_{l_1} : Sp(l_1) \to Sp(\hat{\sigma}(l_1))$, the local correspondence shows too that

$$Spl_1(l_1) = Spl_1(\hat{\sigma}(l_1)) \text{ and } Spl(l) = Spl(\hat{\sigma}(l)).$$

In particular, if l is a Galois extension of $\mathbb{Q}$, Brauer theorem implies that $\hat{\sigma}(l) = l$,

Theorem 2.5.1. ***(Neukirch-Uchida)*** *Let k_1, k_2 be two number fields. The function*

$$\begin{aligned} * : Iso(k_1^{sep}|k_2, k_2^{sep}|k_2) &\to Iso(Gal(k_2^{sep}|k_2), Gal(k_1^{sep}|k_1)) \\ \varphi &\mapsto \varphi^*, \end{aligned}$$

is biyective. In particular, two number fields are isomorphic if, and only if their absolute Galois groups are isomorphic (as profinite groups).

Proof. Without loosing of generality suppose that $k_1^{sep} = k_2^{sep} = \overline{\mathbb{Q}}$. We already show the injectivity of this function.
Let N be finite Galois extension of $\mathbb{Q}$ containing k_1 and k_2, then $\hat{\sigma}(N) = N$, or equivalently σ restricts to an automorphism of $Gal(\overline{\mathbb{Q}}|N)$ and moreover σ induces the next isomorphism

$$\begin{aligned} \sigma^N : Gal(N|k_1) &\to Gal(N|k_2) \\ \theta \circ Gal(\overline{\mathbb{Q}}|N) &\mapsto \sigma(\theta) \circ Gal(\overline{\mathbb{Q}}|N) \end{aligned}$$

$(Gal(\overline{\mathbb{Q}}|k_1)/Gal(\overline{\mathbb{Q}}|N) \simeq Gal(N|k_1))$.
Every $\alpha \in Iso(\overline{\mathbb{Q}}|k_2, \overline{\mathbb{Q}}|k_1)$, induces an isomorphism

$$\begin{aligned} \alpha^* : Gal(\overline{\mathbb{Q}}|k_1) &\to Gal(\overline{\mathbb{Q}}|k_2) \\ \theta &\mapsto \alpha \circ \theta \circ \alpha^{-1} \end{aligned}$$

and, since $\alpha(N) = N$ (N is normal over $\mathbb{Q}$), α^* induces an isomorphism

$$\begin{aligned} (\alpha^*)^N : Gal(N|k_1) &\to Gal(N|k_2) \\ \theta \circ Gal(\overline{\mathbb{Q}}|N) &\mapsto \alpha^*(\theta) \circ Gal(\overline{\mathbb{Q}}|N) \end{aligned}$$

First, we show that there exists $\alpha \in Iso(\overline{\mathbb{Q}}|k_1, \overline{\mathbb{Q}}|k_2)$ such that $(\alpha^*)^N = \sigma^N$, for every Galois extension of $\mathbb{Q}$ containing $k_1 \vee k_2$. We divide the proof of this statement in two cases.

(i) $Gal(N|k_2)$ is cyclic:
Consider the canonical quotient homomorphism

$$f : Gal(\overline{\mathbb{Q}}|k_2) \to Gal(N|k_2),$$

and let β be a generator of $Gal(N|k_2)$. By Chebotarev's density theorem we know that $d_{N,k_2}(\beta)$ is non-empty, therefore there exists a prime P' of N, such that $P' \cap k_2$ is unramified in N, $D(P'|P' \cap \mathbb{Q}) \subseteq Gal(N|k_2)$ and

$$Frob_{P' \cap k_2}^{P'} = \beta,$$

let P be a prime of $\overline{\mathbb{Q}}$ lying over P'. Then, $D(P|P \cap \mathbb{Q}) \subseteq Gal(\overline{\mathbb{Q}}|k_2)$ and

$$f(Frob^{P}_{P\cap k_2}) = Frob^{P'}_{P'\cap k_2} = \beta,$$

in other words, $Frob^{P}_{P\cap k_2} \equiv \beta \pmod{Gal(\overline{\mathbb{Q}}|N)}$.
Neukirch's theorem implies that $\sigma^{-1}(D(P|P\cap\mathbb{Q})) = D(Q|Q\cap\mathbb{Q})$, for some prime Q of $\overline{\mathbb{Q}}$ with $P\cap\mathbb{Q} = Q\cap\mathbb{Q}$. Since $\overline{\mathbb{Q}}$ is a Galois extension of $\mathbb{Q}$, then there exists α an automorphism of $\overline{\mathbb{Q}}$ such that $\alpha(P) = Q$ and therefore $\alpha^{-1}D(P|P\cap\mathbb{Q})\alpha = D(Q|Q\cap\mathbb{Q})$, this implies that

$$Gal(\overline{\mathbb{Q}}|N)D(P|P\cap\mathbb{Q}) = \alpha^*(Gal(\overline{\mathbb{Q}}|N)D(Q|Q\cap\mathbb{Q})).$$

Now, note that $Gal(\overline{\mathbb{Q}}|k_2) = Gal(\overline{\mathbb{Q}}|N)D(P|P\cap\mathbb{Q})$. Indeed, it is clear that $Gal(\overline{\mathbb{Q}}|N)D(P|P\cap\mathbb{Q}) \subseteq Gal(\overline{\mathbb{Q}}|k_2)$. Reciprocally, if $\theta \in Gal(\mathbb{Q}|k_2)$, consider the cannonical quotient homomorphism

$$f : Gal(\overline{\mathbb{Q}}|k_2) \to Gal(N|k_2),$$

since $Gal(N|k_2) = \langle\beta\rangle$, then $F(\theta) = \beta^n$, for some $n \in \mathbb{Z}$, in other words $\theta\circ\beta^{-n} \in Gal(\overline{\mathbb{Q}}|N)$, therefore exists $\theta_1 \in Gal(\overline{\mathbb{Q}}|N)$, such that $\theta = \theta_1\circ\beta^n \in Gal(\overline{\mathbb{Q}}|k_2) \subseteq Gal(\mathbb{Q}|N)D(P|P\cap\mathbb{Q})$ ($\beta^n \in D(P|P\cap\mathbb{Q})$). Thus

$$\begin{aligned}
\alpha^*(Gal(\overline{\mathbb{Q}}|k_1)) &\subseteq Gal(\overline{\mathbb{Q}}|k_2)\\
&= Gal(\overline{\mathbb{Q}}|N)D(P|P\cap\mathbb{Q})\\
&= \alpha^*(Gal(\overline{\mathbb{Q}}|N)D(Q|P\cap\mathbb{Q}))\\
&\subseteq \alpha^*(Gal(\overline{\mathbb{Q}}|k_1)),
\end{aligned}$$

and therefore

$$Gal(\overline{\mathbb{Q}}|k_2) = \alpha^*(Gal(\overline{\mathbb{Q}}|k_1))$$

The fixed field by the group on the left side of previous equation is k_2 and the field fixed by the group on the right side is $\alpha(k_1)$, by Galois theory, $\alpha(k_1) = k_2$. Thus, $\alpha \in Iso(\overline{\mathbb{Q}}|k_1, \overline{\mathbb{Q}}|k_2)$.
Now, we have to show that $(\alpha^*)^N = \sigma^N$. Since $Gal(N|k_1)$ is cyclic with generator β, this is equivalent to show that $(\alpha^*)^N(\beta) = \sigma^N(\beta)$. Let

$$\begin{aligned}
F : D(Q|Q\cap k_1) &\to Gal(\mathcal{O}_l/Q|\mathcal{O}_k/P)\\
\sigma &\mapsto F(\sigma),
\end{aligned}$$

here $F(\sigma)$ is the $\mathcal{O}_l/Q$-automorphism, defined by

$$\begin{aligned}
F(\sigma) : \mathcal{O}_l/Q &\to \mathcal{O}_l/Q\\
x+Q &\mapsto \sigma(x)+Q,
\end{aligned}$$

be the homomorphism defined in the section 2 of this chapter. It is clear that $(\alpha^*)^N(Frob^P_{P\cap k_2)}$ and $\sigma^N(Frob^P_{P\cap k_2)}$ are frobenius elements to, in other words $F((\alpha^*)^N(\beta)) = F(\sigma^N(\beta))$, but Q is unramified (since P is unramified), then F is injective, therefore $(\alpha^*)^N = \sigma^N$.

(ii) $Gal(N|k_2)$ is not cyclic:
Let p be a prime greater than the order of $Gal(N|\mathbb{Q})$. Consider the group ring $\mathbb{F}_p(Gal(N|\mathbb{Q}))$. There exists a finite Galois M extension of $\mathbb{Q}$, containing N, such that there exists an exact sequence

$$1 \to \mathbb{F}_p(Gal(N|\mathbb{Q})) \to Gal(\overline{\mathbb{Q}}|M) \to Gal(N|\mathbb{Q}) \to 1,$$

in the rest of this proof we suppose that $\mathbb{F}_p(Gal(N|\mathbb{Q})) \subseteq Gal(\mathbb{Q}|M)$. In particular, we have the next isomorphism

$$\mathbb{F}_p(Gal(N|k_2)) \simeq Gal(M|N),$$

(see [Neu-Uchi] for details). Since M is a Galois extension of $\mathbb{Q}$, then σ induces an isomorphism

$$\sigma^M : Gal(M|k_1) \to Gal(M|k_2),$$

in particular, identifying $\mathbb{F}_p(Gal(N|\mathbb{Q}))$ with the subgroup $Gal(M|N)$ of $Gal(M|k_2)$ and using the fact that N is a Galois extension of $\mathbb{Q}$, σ^M reestricst to an automorphism of $\mathbb{F}_p(Gal(N|\mathbb{Q}))$, we note this restriction by σ^M_N.
Let $\lambda \in \mathbb{F}_p(Gal(\mathbb{Q})) \setminus \{0\}$, let L_1 be the field, contained in M, fixed by the cyclic subgroup of $\mathbb{F}_p(Gal(N|\mathbb{Q}))$, generated by λ and let L_2 be the field, contained in M, fixed by the cyclic subgroup $\sigma^M(\langle\lambda\rangle)$ of $\mathbb{F}_p(Gal(N|\mathbb{Q}))$. In particular ,we know that $\hat{\sigma}(L_1) = L_2$. Therefore σ restricts to an isomorphism

$$\sigma : Gal(\overline{\mathbb{Q}}|L_1) \to Gal(\mathbb{Q}|L_2).$$

Note that M is a cyclic extension of L_1 and L_2 (its Galois group is clearly cyclic). Then by (i) there exists an automorphism α of $\overline{\mathbb{Q}}$, such that $\alpha(L_1) = L_2$ and $(\alpha^*)^M = \sigma^M$. We want to know how $(\alpha^*)^M$ is defined; recall that α induces an automorphism

$$\begin{aligned} \alpha^* : Gal(\overline{\mathbb{Q}}|k_2) &\to Gal(\overline{\mathbb{Q}}|k_2) \\ \theta &\mapsto \alpha \circ \theta \circ \alpha^{-1}, \end{aligned}$$

In particular, we know that α^* induces an automorphism $(\alpha^*)^M_N$ of $Gal(M|N)$, identifying $Gal(M|N)$ with $\mathbb{F}_p(Gal(N|\mathbb{Q}))$, $(\alpha^*)^M_N$ is then a left multiplication by $h =$

$\alpha^{-1}(mod(Gal(M|N))$. In other words, with the structure of $\mathbb{F}_p(Gal(N|\mathbb{Q}))$ of $Gal(N|k_2)$-module, then

$$\begin{aligned}(\alpha^*)_N^M : \mathbb{F}_p(Gal(N|\mathbb{Q})) &\to \mathbb{F}_p(Gal(N|\mathbb{Q})) \\ g &\mapsto h.g\end{aligned}$$

For each $g \in Gal(N|\mathbb{Q})$, consider the subgroups

$$U_g = \{\lambda \in \mathbb{F}_p(Gal(N|\mathbb{Q}))|\sigma^M(\lambda) = g\lambda\}$$

Using the cyclic case in each element of $\mathbb{F}_p(Gal(N|\mathbb{Q}))$, we can prove that $\bigcup_{g\in Gal(N|\mathbb{Q})} U_g = \mathbb{F}_p(Gal(N|\mathbb{Q}))$. Let $g_0 \in Gal(N|\mathbb{Q})$, such that $|U_{g_0}|$ is maximal in $\{|U_g|\,|g \in Gal(N|\mathbb{Q})\}$. $U_{g_0} = \mathbb{F}_p(Gal(N|k_2))$, indeed, suppose that $U_{g_0} \subsetneq \mathbb{F}_p(Gal(N|\mathbb{Q}))$, since $|\mathbb{F}_p(Gal(N|\mathbb{Q}))| = p^k$, for some $k \in \mathbb{Z}^+$, then $|U_{g_0}| \leq p^{k-1}$, then we have the next

$$\begin{aligned}p^k &= |\mathbb{F}_p(Gal(N|\mathbb{Q}))| \\ &= \left|\bigcup_{g\in Gal(N|\mathbb{Q})} U_g\right| \\ &\leq \sum_{g\in Gal(N|\mathbb{Q})} |U_g| \\ &\leq |Gal(N|\mathbb{Q})||U_{g_0}| \\ &< |Gal(N|\mathbb{Q})|p^{k-1}\end{aligned}$$

a contradiction, since $|Gal(N|\mathbb{Q})| < p$. Then, we can characterize σ_N^M in the next way

$$\begin{aligned}\sigma_N^M : \mathbb{F}_p(Gal(N|\mathbb{Q})) &\to \mathbb{F}_p(Gal(N|\mathbb{Q})) \\ \lambda &\mapsto g_0\lambda\end{aligned}$$

Since $Gal(N|k_1) \subseteq Gal(N|\mathbb{Q})$, we can identify $Gal(N|k_1)$ with a subset of $\mathbb{F}_p(Gal(N|\mathbb{Q}))$, under this identification clearly we have that for each $g_1 \in Gal(N|k_1)$, $\sigma_N^M(g_1) = \sigma^N(g_1)\sigma_N^M(1)$. Following the next equality's

$$g_0g_1 = \sigma_N^M(g_1) = \sigma^N(g_1)\sigma_N^M(1) = \sigma^N(g_1)g_0,$$

we deduce that

$$\sigma^N(g_1) = g_0g_1(g_0)^{-1},$$

or equivalently $\sigma^N = (\alpha^*)^N$.

Thus, in any case we can prove that for every isomorphism $\sigma : Gal(\overline{\mathbb{Q}}|k_1) \to Gal(\overline{\mathbb{Q}}|k_2)$ and for every normal extension N of $k_1 \vee k_2$, there exists an automorphism α_N of $\mathbb{Q}$, such that $\sigma^N = (\alpha_N^*)^N$, then the set

$$\{(\alpha_N^*)^N | N \text{ is a normal extension of } k_1 \vee k_2\}$$

is non-empty and is clearly a projective system whose limit is non-empty. Their limit is the required $\alpha \in Iso(\overline{\mathbb{Q}}|k_2, \overline{\mathbb{Q}}|k_1)$, such that $\alpha = \sigma$ (coincides in every normal extension of $k_1 \vee k_2$). This completes the proof. □

We finish this chapter with a structure result about the absolute Galois groups of the rational numbers $Gal(\overline{\mathbb{Q}}|\mathbb{Q})$.
For number fields k_1 and k_2, define the action

$$\begin{aligned} . : Gal_{k_2} \times Iso(k_2^{sep}|k_2, k_1^{sep}|k_1) &\to Iso(k_2^{sep}|k_2, k_1^{sep}|k_1) \\ (\sigma, \varphi) &\mapsto \varphi \circ \sigma^{-1}, \end{aligned}$$

The coset of this action is $Iso(k_2, k_1)$. Indeed, consider the function

$$\begin{aligned} f : Iso(k_2^{sep}|k_2, k_1^{sep}|k_1) &\to Iso(k_2, k_1) \\ \varphi &\mapsto \varphi|_{k_2}, \end{aligned}$$

Let $\varphi_1, \varphi_2 \in Iso(k_2^{sep}|k_2, k_1^{sep}|k_1)$, satisfying that $f(\varphi_1) = f(\varphi_2)$. Then $\varphi_2^{-1} \circ \varphi_1 \in Gal_{k_2}$ and we have that $\varphi_1 \circ (\varphi_2^{-1} \circ \varphi_1)^{-1} = \varphi_2$, in other words, φ_1 and φ_2 are in the same orbit, reciprocally is trivial that if φ_1 and φ_2 are in the same orbit then $f(\varphi_1) = f(\varphi_2)$. Finally, by the isomorphism extension theorem then f is surjective and the assertion follows.
We introduce a previous definition in order to state and prove an "outer" version of Neukirch-Uchida theorem. Let G be a profinite group and let $Aut(G)$ be the group of continuous automorphisms of G. The function

$$\begin{aligned} Inn : G &\to Aut(G) \\ g &\mapsto Inn(g) \end{aligned}$$

is a continuous group homomorphism, where $Inn(g)(x) = g^{-1}xg$, for every $x \in G$. φ_g is called the ***inner automorphism*** of G, induced by g. The subgroup $Inn(G)$ of $Aut(G)$ is called the ***group of inner automorphisms*** of G.
Let G_1 and G_2 be profinite groups, denote by $Iso(G_1, G_2)$ to be the set of continuous group isomorphisms from G_1 to G_2, then $Inn(G_2)$ acts on this set, define the continuous action

$$\begin{aligned} . : Inn(G_2) \times Iso(G_1, G_2) &\to Iso(G_1, G_2) \\ (\varphi, \sigma) &\mapsto \sigma \circ \varphi, \end{aligned}$$

Definition 2.5.1. *Let G_1 and G_2 be profinite groups* ***the set of exterior isomorphisms*** *of G_1 to G_2 is the quotient set $Iso(G_1, G_2)/Inn(G_2)$, this set is denoted by $OutI(G_1, G_2)$. An element of $Out(G_1, G_2)$ is called an* ***exterior isomorphism*** *from G_1 to G_2.*

Corollary 2.5.3. *Let k_1 and k_2 be number fields. There exists a bijection*

$$Iso(k_2, k_1) \simeq Out(Gal_{k_1}, Gal_{k_2}).$$

Proof. Let $\sigma \in Gal_{k_2}$ and $\varphi \in Iso(\overline{k_2}|k_2, \overline{k_1}|k_1)$

$$\begin{aligned} .(\sigma, \varphi)^* &= (\varphi \circ \sigma^{-1})^* \\ &= \varphi^* \circ Inn(\sigma), \end{aligned} \tag{2-1}$$

or equivalently, the next diagram is commutative

$$\begin{array}{ccc} Gal_{k_2} \times Iso(\overline{k_2}|k_2, \overline{k_1}|k_1) & \longrightarrow & Iso(\overline{k_2}|k_2, \overline{k_1}|k_1) \\ \downarrow{\scriptstyle Inn \times *} & & \downarrow{\scriptstyle *} \\ Inn(Gal_{k_2}) \times Iso(Gal_{k_1}, Gal_{k_2}) & \longrightarrow & Iso(Gal_{k_1}, Gal_{k_2}) \end{array}$$

By Neukirch-Uchida theorem the vertical arrows are bijective. Thus,

$$Iso(\overline{k_2}|k_2, \overline{k_1}|k_1)/Gal_{k_2} \simeq Iso(Gal_{k_1}, Gal_{k_2})/Inn(Gal_{k_2}).$$

Or equivalently,

$$Iso(k_2, k_1) \simeq Out(Gal_{k_1}, Gal_{k_2}).$$

□

Corollary 2.5.4. *All continuous automorphisms of $Gal_{\mathbb{Q}}$ are inner.*

$Out(Gal_{\mathbb{Q}}, Gal_{\mathbb{Q}}) \simeq Iso(\mathbb{Q}, \mathbb{Q})$, but $Iso(\mathbb{Q}, \mathbb{Q})$ is the trivial group. Then $Out(Gal_{\mathbb{Q}}, Gal_{\mathbb{Q}})$ is trivial and therefore $Aut(Gal_{\mathbb{Q}}) = Inn(Gal_{\mathbb{Q}})$.

3 Étale fundamental group

In this chapter we introduce the definition of the étale fundamental group, properties and consequences. First, we study some characterizations of the first fundamental group for some topological spaces with certain properties, in this situation, the first fundamental group can be described in three different ways. We introduce étale morphisms between schemes, we give examples and some descriptions, using this type of morphisms we introduce finite étale coverings of a scheme and we construct with this covers finite étale groups.

3.1 The topological fundamental group

Let X be a topological space and $x \in X$.

Definition 3.1.1. *The first fundamental group of X based in x, denoted by $\pi_1(X,x)$, is the set of homotopy classes of loops in X based at x.*

$\pi_1(X,x)$ is a group with the concatenation operation in homotopy classes of loops. If $x, y \in X$, then a path from x to y, produces a group isomorphism from $\pi_1(X,x)$ to $\pi_1(X,y)$. Therefore, for a path connected space X we can associate an algebraic invariant, denoted by $\pi_1(X)$, defined as the first fundamental group of some point $x \in X$. X is said to be simply connected if it is path connected and $\pi_1(X) = 0$, and semilocally simply connected if for every $x \in X$, there exists an open simply connected subset containing x.
The theory of the fundamental group are related with the theory of covering spaces. Recall, a covering space $p : Y \to X$ is a continuous function, such that for every $x \in X$, there exists an open set U of X, containing x, open subsets V_i of Y

$$p^{-1}(U) = \coprod_{i \in I} V_i,$$

and the restriction $p|_{V_i} : V_i \to U$ is an homeomorphism. We denote by Cov_X the category of covering spaces over X.
Let $p : Y \to X$ be a covering space. If we fix an element $y \in p^{-1}(x)$, then every loop γ can be lifted to a unique path γ_y in Y, such that $\overline{\gamma}(0) = y$. Moreover, if γ and η are two homotopic loops of X based at x, their lifts (with initial point y) γ_y, η_y are homotopic, in particular, γ_y and η_y have the same end point. This allow us, to define the next action

$$\begin{aligned} . : \pi_1(X,x) \times p^{-1}(x) &\to p^{-1}(x) \\ ([\gamma], y) &\to \gamma_y(1) \end{aligned}$$

This action is called the *monodromy action*. We denote by $\pi_1(X,x)-$sets the category of sets with an action of the fundamental group and morphisms functions compatible with this actions.

Theorem 3.1.1. ***(Classification of covering spaces)*** *Let X be a path-connected, locally path-connected and semi-locally simply-connected topological space. The functor*

$$\begin{aligned} Fib_x : Cov_X &\to \pi_1(X,x) - sets \\ (q : Y \to X) &\mapsto q^{-1}(x) \end{aligned}$$

is an equivalence of categories.

In the rest of this section we suppose that X is path connected, locally path connect and semi-locally simply-connected. The previous theorem classifies covering spaces over X in terms of the monodromy action of $\pi_1(X,x)$, in particular, we have that the group $Aut(Fib_x)$ of natural automorphisms of Fib_x is isomorphic to $\pi_1(X,x)$.
There exists a covering space $q : \widetilde{X} \to X$, such that for every covering space $p : Y \to X$, with Y connected, there exists a covering $f : \widetilde{X} \to Y$, such that $q = p \circ f$. This covering space is called the *universal covering space* of X and is determined up to isomorphisms of covering spaces.

Theorem 3.1.2. *Let X be a path-connected, locally path-connected and semi-locally simply connected topological space. The functor*

$$Fib_x : Cov_X \to \pi_1(X,x),$$

is representable, represented by the universal covering of X. In other words, if $\widetilde{X}$ is the universal covering of X, then we have a natural isomorphism $Hom(\widetilde{X}, \_) \simeq Fib_x$.

In particular, the previous theorem implies that $\pi_1(X,x) = Aut(\widetilde{X}|X)$, where $Aut(\widetilde{X}|X)$ is the groups of deck transformation of the universal covering $\widetilde{X}$ over X.
In one hand, since Fib_x is an equivalence of categories, we have one description of the fundamental group using natural automorphisms of the fiber functor Fib_x, in the other hand we have a description of the fundamental group using deck transformations of the universal cover. In the next chapter we will see how this descriptions allow us to define the fundamental group in the algebro-geometric setting.
A covering space $f : X \to Y$ the cardinality of the fibers does not change point by point, to be precise if $x, y \in Y$, then $—f^{-1}(x)| = |f^{-1}(y)|$. This allow us to define the notion of *finite covering space*, to be a covering space such that the one fiber is a finite set (and therefore all fiber is a finite set). Denote by $FCov_X$ be the category of finite covering space and for a point $x \in X$, define the next fiber functor

$$\begin{aligned} G_x : FCov_X &\to Sets \\ (q : Y \to X) &\mapsto q^{-1}(x). \end{aligned}$$

For X path-connected, locally path-connected and semi-locally simply-connected we have the next relation between $Aut(G_x)$ and the first fundamental group

$$G_x \simeq \pi_1(\hat{X}, x),$$

where $\pi_1(\hat{X}, x)$ means the profinite completion of $\pi_1(X, x)$ (the inverse limit of the finite quoutients of $\pi_1(X, x)$)

3.2 Étale morphisms

étale morphisms unifying several concepts coming from algebra, geometry, topology, number theory and so on, some examples are given in this section. This definition was introduced by Grothendieck in [9] to study a cohomology theory of varieties over finite fields that satisfies de Wéil axioms, called étale cohomology. In this text we do not discuss this theory, we are only interested in the fundamental-group theory of the étale morphisms and his relation with arithmetic. étale cohomology theory can be studied in [24].
In the previous section we see that for a special-type of topological spaces X, we have isomorphisms between the next three groups

(i) $\pi_1(X, x)$ or the group of loops based at x, up to homotopy.

(ii) $Aut(Fib_x)$ or the group of natural isomorphisms of the fiber functor Fib_x.

(iii) $Aut(\widetilde{X}|X)$ or the group of deck transformations of some universal covering $\widetilde{X}$ of X.

We want to define an analogue to the fundamental group in algebraic geometry that bring us results that coincides with our algebro-geometric intuition. We have three possible choices to do this, corresponding to the three previous description of the same group. So we have to clarify the requirements of each definition

(i) The usual definition of the fundamental group requires the notion of loops.

(ii) The second definition requires the notion of covering space in the algebro-geometric setting.

(iii) The last definition requires the notion of covering space and the existence of a universal covering space.

We have three natural questions corresponding to this three requirements

The loops of an algebraic variety or a scheme are good enough?

What it means a covering space in algebraic geometry?

There exists a universal covering space over any scheme?

The loops in an algebraic variety does not correspond in many cases to a subvariety, we refer to the cases when the dimension of this object is 1/2. We abandon this approach to the fundamental group.
One idea to understand how to define covering spaces in algebraic geometry is to see one place where algebraic geometry and topology meets: the case of complex varieties, intuitively we want that if $f : X \to Y$ is a morphism between non-singular complex algebraic varieties, then f is an "algebraic covering space" if, and only if the analytification f^{an} of f is a covering space in the usual sense.
For example, consider the morphisms of algebraic varieties

$$\begin{aligned} f_k : \mathbb{A}^1_{\mathbb{C}} &\to \mathbb{A}^1_{\mathbb{C}} \\ z &\mapsto z^k, \end{aligned}$$

for every $k \in \mathbb{Z}^+$. The analytification of the previous morphism is the map between complex manifolds

$$\begin{aligned} g_k : \mathbb{C} &\to \mathbb{C} \\ z &\mapsto z^k \end{aligned}$$

this maps are not covering spaces, because they have a ramification point, namely 0. Therefore, f_k does not deserves the name of "algebraic covering space". But the map

$$\begin{aligned} h_k : \mathbb{C} \setminus \{0\} &\to \mathbb{C} \setminus \{0\} \\ z &\mapsto z^k, \end{aligned}$$

is a covering space of $\mathbb{C} \setminus \{0\}$. Then

$$\begin{aligned} f_k : \mathbb{A}^1_{\mathbb{C}} \setminus \{0\} &\to \mathbb{A}^1_{\mathbb{C}} \setminus \{0\} \\ z &\mapsto z^k, \end{aligned}$$

deserves the name of "algebraic covering space". But the universal cover space of $\mathbb{C} \setminus \{0\}$ is the exponential map

$$\begin{aligned} g : \mathbb{C} &\to \mathbb{C} \setminus \{0\} \\ x &\mapsto e^x. \end{aligned}$$

But, g is not the analytification of any morphism from $\mathbb{A}^1_{\mathbb{C}}$ to $\mathbb{A}^1_{\mathbb{C}} \setminus \{0\}$ (intuitively: is not algebraic). Therefore, the algebraic variety $\mathbb{A}^1_{\mathbb{C}} \setminus \{0\}$ does not have an universal covering. Then in general, we do not have existence of "universal algebraic covering maps". This shows that the unique reasonable way to define the fundamental group in the algebro-geometric sense is to make sense what precisely means "algebraic covering space". The key ingredients of this definition are three: flat, finite-type and unramified.

Definition 3.2.1. *Let $\varphi : X \to Y$ be a morphism of schemes. We say that φ is **flat at** $x \in X$ is the induced morphism in stalks $\varphi_x^* : \mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}$ is a flat map of rings (i.e., with the structure induced by φ_x^*, $\mathcal{O}_{X,x}$ is a flat $\mathcal{O}_{Y,\varphi(x)}$-module). We say that φ is **flat** if it is flat at every point of X.*

The notion of flat morphism is related with the idea of a family of geometric objects variously in a continuous way.

Definition 3.2.2. *Let $\varphi : X \to Y$ be a morphisms of schemes. We say that φ is **of finite type** if there exists an affine open cover $\{Spec(A_i)\}_{i\in I}$ of Y, such that for every $i \in I$, there exists an affine open cover $\{Spec(B_{i,j})\}_{j\in J_i}$ of $\varphi^{-1}(Spec(A_i))$, such that the induced map of rings $A_i \to B_{i,j}$ is of finite type (i.e., $B_{i,j}$ is a finitely generated A_i-algebra).*

Notice that the finite type condition on a morphism φ is an example of a affine communication property, i.e., is φ is a morphism of finite type then for every affine open cover $\{Spec(A_i)\}_{i\in I}$ of Y and for every open cover $\{Spec(B_{i,j})\}_{j\in J_i}$ of $\varphi^{-1}(Spec(A_i))$, the infuced maps of rings $A_i \to B_{i,j}$ is of finite type.

Definition 3.2.3. *Let $\varphi : X \to Y$ be a morphism of schemes. We say that φ is **unramified at** $x \in X$ if*

(i) $\mathfrak{m}_x = \varphi_x^*(\mathfrak{m}_{\varphi(x)})\mathcal{O}_{X,x}$, i.e., the ideal generated by $\varphi_x^*(\mathfrak{m}_{\varphi(x)})$ in $\mathcal{O}_x$ is equal to the maximal ideal of $\mathcal{O}_x$, where $\mathfrak{m}_{\varphi(x)}$ is the maximal ideal of $\mathcal{O}_{Y,\varphi(x)}$.

(ii) $\mathcal{O}_{X,x}/\mathfrak{m}_x$ is a separable extension of $\mathcal{O}_{Y,\varphi(x)}/\mathfrak{m}_{\varphi(x)}$.

*We say that φ is **unramified** if it is unramified at every point of X.*

Definition 3.2.4. *Let $\varphi : X \to Y$ be a morphism of schemes. We say that φ is **étale at** $x \in X$ is if it is flat at x, of finite type and unramified at x. We say that φ is **étale** if it is étale at every point of X.*

Let k be an algebraically closed field. The étale morphisms between non-singular algebraic varieties have an equivalent condition, related with the hypothesis of the theorem of the inverse function map of vector calculus. For general algebraic varieties (with singular points or not), we have an equivalent notion in terms of the $\mathfrak{m}$-adic completion of stalks, in the two cases the étale morphisms incarnate the idea of preserve local analytic information. To be precise:
Let $\varphi : X \to Y$ be a morphism betweeen non-singular algebraic varieties, then φ is étale if and only if for every point $x \in X$ the application between tangent spaces $df_x : T_x(X) \to T_{\varphi(x)}(Y)$ is a linear isomorphism.
For example, for every $j \in \mathbb{Z}^+$ with $j \neq char(k)$, the map

$$\begin{aligned} f_j : \mathbb{A}^1_{\mathbb{C}} &\to \mathbb{A}^1_{\mathbb{C}} \\ z &\mapsto z^j, \end{aligned}$$

is étale at every point non-zero point z. Because for every $z \in \mathbb{A}^1_{\mathbb{C}}$

$$\begin{aligned} d(f_k)_z : T_z(\mathbb{A}^1_{\mathbb{C}}) &\to T_{z^k}(\mathbb{A}^1_{\mathbb{C}}) \\ v &\mapsto (jz^{j-1})v \end{aligned}$$

is a linear isomorphism, unless $z = 0$.
Recall that the condition of isomorphisms on the tangent spaces are equivalent to local diffeomorphisms in differential geometry.
For general varieties we have that a morphism $\varphi : X \to Y$ is étale at $x \in X$ if and only if the induced morphism

$$\bigoplus_{i\in\mathbb{N}} m^n_{\varphi(x)}/m^{n+1}_{\varphi(x)} \to \bigoplus_{i\in\mathbb{N}} m^n_x/m^{n+1}_x$$

is an isomorphism. Notice that, this is equivalent to the inducen morphism between the $\mathfrak{m}$-adic completions of the rings $\mathcal{O}_{Y,\varphi(x)}$ and $\mathcal{O}_{X,x}$ is an isomorphism. In particular, there no exists étale morphisms between algebraic varieties of different dimension.
We give another example coming from algebraic number theory. Let k be a number field , then the inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_k$, induces an scheme morphisms

$$\varphi : Spec(\mathcal{O}_k) \to Spec(\mathbb{Z}),$$

φ is of finite type and flat because $\mathcal{O}_k$ is a free finitely generated $\mathbb{Z}-$module, and for every prime ideal P of $\mathcal{O}_k$, the residue field $\mathcal{O}_{k,P}/\mathfrak{m}_P$ is a separable extension of $\mathbb{Z}_{\varphi(P)}/\mathfrak{m}_\varphi(P)$. Indeed, if $P \neq 0$, then is just a extension of finite fields and thus separable, if $P = 0$, then this extension is $k|\mathbb{Q}$ which is separable. Thus, $\varphi : Spec(\mathcal{O}_k) \to Spec(\mathbb{Z})$ is étale if and only if $\mathfrak{m}_P = \varphi^*_P(\mathfrak{m}_{\varphi(P)})\mathcal{O}_{k,P}$. Let $Q = \varphi(P) = P \cap \mathbb{Z}$, or equivalently, if the next two localization of ideals in P are equal $P_P = (\varphi(P)\mathcal{O}_k)_P$. Let

$$\varphi(P)\mathcal{O}_k = Q_1^{e_1}...Q_r^{e_r},$$

be the factorization of Q as a product of prime ideals in $\mathcal{O}_k$, as $\varphi(P) = Q$, then P is lying over Q (φ is induced by the inclusion map of rings), therefore $P = Q_i$ for some $i \in \{1, ..., r\}$. If the ramification index $e(P|\varphi(P)) > 1$, then we have the next strict inclusion of localized ideals

$$(\varphi(P)\mathcal{O}_k)_P = (P^{e(P|Q)})_P \subsetneq P_P,$$

and reciprocally if $(Q\mathcal{O}_k)_P = P_P$, then $e(P|Q) = 1$. Therefore φ is étale at P if and only if $\varphi(P|\varphi(P)) = 1$, in other words, if and only if P is unramified over $\varphi(P)$.
Another example given, this time coming from geometry, if $f : Y \to X$ is a holomorphic map between connected and compact riemann surfaces $\mathcal{O}_Y$, $\mathcal{O}_X$ are the sheaf of holomorphic functions of Y, X, respectively, and $\mathcal{M}(Y), \mathcal{M}(X)$ are the field of meromorphic functions of Y, X, respectively. Let $x \in X$, we have that $\mathcal{O}_{X,x}$ is a subring of $\mathcal{M}(X)$ and $\mathcal{M}(Y)$ is a finite

extension of $\mathcal{M}(X)$. Let B be the integral closure of $\mathcal{O}_X(X)$ in $\mathcal{M}(Y)$, B is a Dedekind domain provided that the stalk at a point x of X, $\mathcal{O}_{X,x}$ is a discrete valuation ring (the valuation is the order of zero or pole of a meromorphic function at x). The unique non-zero prime ideal of $\mathcal{O}_{X,x}$ is

$$\mathfrak{m}_x = \{\langle \varphi, U\rangle \in \mathcal{O}_{X,x} | \varphi(x) = 0\},$$

then the next three properties are equivalent

(i) f is unramified at x (in the sense of Riemann surfaces).

(ii) $\mathfrak{m}_x$ is unramified in B (in the sense of algebraic number theory).

(iii) The induced map $Spec(B) \to Spec(\mathcal{O}_{X,x})$ is étale at $\mathfrak{m}_x$.

One special case where we study the étale condition is in the case of a field. Let $\varphi : Spec(A) \to Spec(k)$ be a étale morphism with k be a field and A be any ring. Let $P \in Spec(A)$, therefore $\varphi(P) = (0) \in Spec(k)$, as φ is unramified, then

$$P_P = \varphi_P^*((0))A_P = (0)$$

therefore, no prime ideal is contained in P, in other words, $Spec(A)$ is a discrete space and by compactness it is a finite discrete space, since A is a finitely generated k-algebra by Hilbert's basis theorem we have that A is Noetherian, thus A is Artinian and therefore

$$\begin{aligned} A &\simeq \prod_{P \in Spec(A)} A_P \\ &\simeq \prod_{P \in Spec(A)} A_P/P_P, \end{aligned}$$

since φ is unramified, then A_P/P_P is a separable field extension of k.
Reciprocally, is clear that if A is an étale k-algebra then the induced morphism $\varphi : Spec(A) \to Spec(k)$ is étale. Therefore, makes sense the next definition.

Definition 3.2.5. *Let k be a field. A k-algebra A is **étale** is A is isomorphic to a finite product of separable field extensions of k.*

For example, let $f : X \to \mathbb{P}^1_{\mathbb{C}}$ be a holomorphic non constant function, where X is a compact Riemann surface and $\mathbb{P}^1_{\mathbb{C}}$ is the Riemann sphere, then the ring of meromorphic functions of X is an étale $\mathbb{C}(t)$-algebra. The pullback $f^* : \mathbb{C}(t) = \mathcal{M}(\mathbb{P}^1_{\mathbb{C}}) \to \mathcal{M}(X)$ is a ring homomorphism and if $\{Y_i\}_{i=1}^n$ are the connected components of X, the next two rings are isomorphic:

$$\mathcal{M}(X) \simeq \prod_{i=1}^{n} \mathcal{M}(Y_i),$$

for each $i \in \{1, ..., n\}$, Y_i are compact and connected Riemann surfaces, therefore $\mathcal{M}(Y_i)$ are fields of characteristic zero, thus separable extensions of $\mathbb{C}(t)$.
The proof of the next two statements are routine and will not be discussed here, for details see, for example, [24].

Proposition 3.2.1. *(i) Open immersions are étale.*

(ii) The composition of two étale morphisms is étale.

(iii) étale morphisms are stable under base change.

Proposition 3.2.2. *Let $\varphi : X \to Y$, $\psi : Y \to Z$. If ψ is étale and $\psi \circ \varphi$ is étale, then φ is étale.*

3.3 Finite étale coverings

In this section we define the correct algebro-geometric analogue to the notion of covering space, the called finite étale coverings we explore some topological consequences and finally the Galois theory of this coverings, not all the theory of this coverings is discussed here, for more on this coverings see [49].

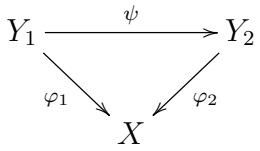
Definition 3.3.1. *A morphism $\varphi : X \to Y$ of schemes is called **finite** if for every affine open subset $Spec(A)$ of Y, we have that $\varphi^{-1}(Spec(A)) = Spec(B)$ is an affine open subset of X and the induced morphism $A \to B$ is finite, i.e., B is a finitely generated A-module. We say that φ is **finitely presented** if $A \to B$ is finitely presented, i.e., B is a finitely presented A-module.*

The composition of two finite (respectively finitely presented) morphisms is a finite (respectively finitely presented) morphism and the change base of every finite morphisms (respectively finitely presented) is finite (respectively finitely presented). As every finitely presented module is, in particular, a finitely generated module, then every finitely presented morphism between schemes is finite. The converse holds for morphisms between locally noetherian schemes.
As an example of finite morphisms we have that any closed immersion is a finite morphism, and every finite morphism is closed (for details in the proofs see [24]).

Definition 3.3.2. *A morphism $\varphi : Y \to X$ of schemes is a **finite étale covering** of X, is a finitely presented, étale and surjective morphism of schemes.*

Of course, if we only work with locally noetherian schemes, then a finite étale covering is the same as a surjective finite and étale morphism, in the general case, we have to work with this extra assumption.

For a scheme X, let $F\acute{E}t_X$ be the category of finite étale coverings of X, i.e., an object in $F\acute{E}t_X$ is a finite étale covering $\varphi : Y \to X$, a morphism in $F\acute{E}t_X$ from $\varphi_1 : Y_1 \to X$ to $\varphi_2 : Y_2 \to X$ is an scheme morphism $\psi : Y_1 \to Y_2$, such that the next diagram is commutative



A finite étale covering is in particular affine. Then if $\varphi : X \to Spec(k)$ is a finite étale covering of X, then X is affine, let $X = Spec(A)$, since φ is in particular étale, we know that A is a k-algebra étale, equivalently $A \simeq \prod_{i=1}^{n} k_i$, where k_i is a separable extension of k. As φ is in particular finite, then k_i is a finite k-module, or equivalently a k_i finite separable extension of k. We say than a k-algebra A is finite étale if $A \simeq \prod_{i=1}^{n} k_i$, where k_i are finite and separable extensions of k. Reciprocally if A is a finite étale k-algebra, then $Spec(A) \to Spec(k)$ is a finite étale covering. Denote by $F\acute{E}t_k$ be the category of finite étale k-algebras. Restricting the equivalence $Spec$ we have the next result.

Theorem 3.3.1. *The functor $Spec : F\acute{E}t_k \to F\acute{E}t_{Spec(k)}$ is an equivalence of categories.*

For any scheme X and any field k, we denote by $X(k)$ the set of k-rational points of X, i.e., $X(k) = Hom(Spec(k), X)$. For example, if X is a non-singular $\mathbb{C}$-variety, then $X(\mathbb{C})$ is a complex manifold.
The next beautiful theorem show us a deep connection between finite étale coverings and finite cover spaces in the complex case and his proof can be found in [9].

Theorem 3.3.2. ***(Grothendieck-Riemann existence theorem)***
If X is a $\mathbb{C}$-variety, then for every finite étale covering $\varphi : Y \to X$, the map $\varphi(\mathbb{C}) : Y(\mathbb{C}) \to X(\mathbb{C})$ is a finite covering space. Moreover, the functor

$$Hom(Spec(\mathbb{C}), \_) : F\acute{E}t_X \to FCov_{X(\mathbb{C})},$$

is an equivalence of categories.

First, we explore some properties of finite étale coverings, then the notion of geometric point and some topological relations with finite étale covers.

Definition 3.3.3. *A morphisms $\varphi : X \to Y$ is said to be **separated** if the induced morphism $\Delta : X \to X \times_Y X$ is a closed immersion.*

We know that the Zariski topology in some schemes, for example varieties, is too coarse to have good separation properties in the usual sense of topology, like the Hausdorff axiom of separation. Again, in the case of varieties over a closed field rarely a variety is Hausdorff (only the finite points), however they satisfies that the structure morphism over its ground field its separated, separated morphisms play the role of the Hausdorff axiom in schemes and reflects the intuitive idea that the varieties satisfies a separation property of points, not in the classical topological sense but in the algebraic geometric sense.

Proposition 3.3.1. *Let $\varphi : Y \to X$ and $\psi : X \to Z$ be morphisms of schemes. If $\psi \circ \varphi$ is fnite and ψ is separated, then φ is finite.*

Proof. Since ψ is separated, then the induced morphism $\Delta : X \to X \times_Z X$ is a closed immersion. In particular, it is finite, then the base change

$$\Delta \times_X id_Y : X \times_X Y \to (X \times_Z X) \times_X Y,$$

is finite too. But the previous morphism is isomorphic to the graph morphism

$$\Gamma_\varphi : Y \to Y \times_Z X$$

and therefore Γ is finite. On the other hand, considering the next tensor product

$$\begin{array}{ccc} Y \times_Z X & \xrightarrow{p_2} & X \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle \psi} \\ Y & \xrightarrow[\psi \circ \varphi]{} & Z \end{array}$$

by hypothesis $\psi \circ \varphi$ is finite and therefore p_2 is finite. But $\varphi = p_2 \circ \Gamma_\varphi$ and therefore φ is finite. □

Proposition 3.3.2. *Let $\varphi : Y \to X$ be a finite étale covering of X. If $s : X \to Y$ is section of φ, then s is an isomorphism between X and some closed and open subscheme of Y. In particular, if X is connected, then φ is an isomorphism of X with some connected component of Y.*

Proof. Since φ and $\varphi \circ s = id_X$ are finite étale, then s is finite étale. Then the image of s is open because s is étale and since s is a finitely presented morphism, then the image of s is closed. Let $Z = s(X)$ be the open and closed subscheme of S (with its canonical structure as an open subscheme), then $\varphi : X \to Z$ is an isomorphism, with inverse $s|_Z : Z \to X$. □

Definition 3.3.4. *Let X be an scheme. A **geometric point** of X is a morphism $\overline{x} : Spec(k) \to X$, where k is an algebraically closed field.*

The geometric points of an scheme X can not identified with points of X, but also identified with points $x \in X$ and inclusion of the residual field $k(x)$ of x into k, an algebraically closed field. For details see [Hartshorne Exercise]. Once we introduce this class of points we have to justify the reason of their introduction and define how to evaluate in this points, what it mean the fiber on a geometric point, etc.
If $\varphi : Y \to X$ is a morphism of schemes and $\overline{y} : Spec(l) \to Y$ is a geometric point, then the evaluation of φ in $\overline{y}$, denoted by $\varphi(\overline{y})$, is the composition of morphisms $\varphi \circ \overline{y}$.

Proposition 3.3.3. *Let Z be a X-connected scheme and $\varphi_1, \varphi_2 : Z \to Y$ be finite étale X-morphisms. If $\varphi_1(\overline{z}) = \varphi_2(\overline{z})$, for some geometric point $\overline{z} : Spec(k) \to Z$, then $\varphi_1 = \varphi_2$.*

Proof. We can assume that $Z = X$, otherwise we can take the change base of all the morphisms involved by Z and the resultant morphisms satisifies the same hypothesis, since finite étale morphisms are stable under base change. Under this assusmption φ_1, φ_2 are two Z-morphisms, then they are sections of the structure morphism $Y \to Z$, therefore they are isomorphisms between Z and a connected component of Y, since Z is connected. But by hypothesis they coincide at least in one point and therefore $\varphi_1(Z) = \varphi_2(Z)$. Thus, the composition $\varphi_1^{-1} \circ \varphi_2 : Z \to Z$ makes sense and moreover is an Z-automorphism of Z, hence it is the identity automorphism of Z, in other words, $\varphi_1^{-1} \circ \varphi_2 = id_S$ and finally $\varphi_1 = \varphi_2$ □

Definition 3.3.5. *Let $\varphi : Y \to X$ be a morphism of schemes and $\overline{x} : Spec(k) \to X$ be a geometric point of X. The **geometric fiber** of $\overline{x}$ in Y, denoted by $Y_{\overline{x}}$, is the scheme $Y \times_X Spec(k)$.*

In the same situation of the last definition if (0) is the unique point of $Spec(k)$ and $x = \overline{x}(0)$, the geometric fiber $Y \times_X Spec(k)$ has underlying topological space homeomorphic to $\varphi^{-1}(x)$. Some topological properties of the geometric fiber $Y_{\overline{x}}$ can be thinking in terms of the topological fiber $\varphi^{-1}(x)$.
Let X be a S-scheme, we denote by $Aut(X|S)$ be the group of S- automorphisms of X. The natural action of $Aut(X|S)$ can be carried to any geometric fiber. For every geometric point $\overline{s} : Spec(k) \to S$ of S, define the action

$$\begin{aligned} . : Aut(X|S) \times X_{\overline{s}} &\to X_{\overline{s}} \\ (\sigma, y) &\mapsto \sigma_s(y), \end{aligned}$$

where $\sigma_s : X_{\overline{s}} \to X_{\overline{s}}$ is the base change of the automorphism σ. If $\varphi : X \to S$ is the structure morphism of X and $s = \overline{s}((0))$, then this action identifies with

$$\begin{aligned} . : Aut(X|S) \times \varphi^{-1}(s) &\to \varphi^{-1}(s) \\ (\sigma, y) &\mapsto \sigma(y). \end{aligned}$$

Note the similarity of the action define below and the natural action of the Galois group in a separable extension of fields, and the similarity with this action with the action of decks transformations in a covering space.

Proposition 3.3.4. *If $\varphi : X \to S$ is a connected finite étale covering then $Aut(X|S)$ acts freely in geometric fibers, i.e., the unique element of $Aut(X|S)$ that fixes one point in the geometric fiber is the identity element.*

Proof. Let $\overline{s} : Spec(k) \to S$ be a geometric point, and s be the associated point in S. If $\sigma \in Aut(X|S)$ satisfies that $\sigma(y) = y$, for some $y \in \varphi^{-1}(s)$ then consider the algebraic closure $\overline{k(y)}$ of the residual field of y. We can construct the geometric point $\overline{y} : Spec(\overline{k(y)} \to X$ of X and note that $\varphi(\overline{y}) = id_X(\overline{y})$, therefore $\varphi = id_X$. □

Corollary 3.3.1. *If $\varphi : X \to S$ is a connected, finite étale covering, then $Aut(X|S)$ is finite.*

Proof. Let $\overline{s} : Spec(k) \to S$ be a geometric point of S and s be the associated point of S. Fixing a point $x \in \varphi^{-1}(s)$, consider the function

$$\begin{aligned} f : Aut(X|S) &\to \varphi^{-1}(s) \\ \sigma &\mapsto \sigma(x), \end{aligned}$$

the previous proposition implies that f is injective and as $\varphi^{-1}(s)$ is finite (since φ is finite and therefore quasi-finite), then the assertion follows. □

Following the similarity between the finite étale coverings of a scheme and the separable extension of a field (or even the similarity with covering spaces), we define Galois objects in the category of $F\acute{E}t_X$, we will see how deep is this similarity and some beautiful consequences of this connections.

Definition 3.3.6. *A connected finite étale covering $\varphi : X \to S$ is called a Galois covering of S if $Aut(X|S)$ acts transitively in each geometric fiber.*

The next theorem justify why introduce geometric points, instead of work with classical points: The fiber in geometric points does not change point by point. This remind us a similar situation in algebraic topology.

Proposition 3.3.5. *Let $\varphi : X \to S$ be a connected finite étale covering of S. If $\overline{s_1} : Spec(k_1) \to S$ and $\overline{s_2} : Spec(k_2) \to S$ are two geometric points, then the cardinal numbers of the geometric fibers $X_{\overline{s_1}}$ and $X_{\overline{s_2}}$ are equal.*

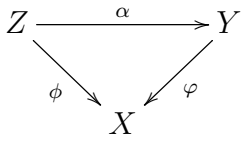
Definition 3.3.7. *The index of a connected, finite, étale covering is the cardinal number of one (all) geometric fiber.*

Note that the index of a connected, finite, étale covering is always a natural number because the cardinal number of the fiber is always a natural number. Also, if $\varphi : X \to S$ is a connected, finite and étale covering of S, then X is a Galois covering of S if and only if $Aut(X|S)$ acts transitively in one geometric fiber. Indeed, one direction is trivial, for the other one if we suppose that $Aut(X|S)$ acts transitively in one geometric fiber, for example in $X_{\overline{s}}$, for some geometric point $\overline{s} : Spec(k) \to S$, fixing a point $x \in X_{\overline{s}}$, then the function

$$\begin{aligned} f : Aut(X|S) &\to \varphi^{-1}(s) \\ \sigma &\mapsto \sigma(x) \end{aligned}$$

is not only injective, in addition it is surjective, therefore $Aut(X|S)$ have cardinal number equal to the index of φ and therefore X is Galois (in any case φ acts freely in fibers).
Recall that any separable extension of a fields have a Galois closure, in the sense that is the minimal Galois extension containing a separable extension. The same is true in the case of scheme theory.

Proposition 3.3.6. *If $\varphi : X \to S$ is connected, finite and étale covering of S, then there exists $\psi : Y \to X$ a Galois covering of X, such that $\varphi \circ \psi : Y \to S$ is a Galois covering of S and the next universal property holds: For every connected, finite and étale covering $\phi : Z \to X$ of X if $\varphi \circ \phi : Z \to S$ is a Galois covering of S, then there exists a unique finite étale morphisms $\alpha : Z \to Y$ such that the next diagram is commutative*



*Y is unique up to isomorphisms and is called the **Galois closure** of $\varphi : X \to S$.*

Proof. Let $\overline{s} : Spec(k) \to S$ be a geometric point of S, as $\varphi : X \to S$ is, in particular finite, then it is quasi-finite and therefore the geometric fiber $X \times_S Spec(k)$ has a finite number of elements. Let $\overline{x}_1, ...\overline{x}_n$, be such elements, in other words, for every $i \in \{1, ..., n\}$ we have a geometric point

$$\overline{x}_i : Spec(k) \to X,$$

and denote by $x_i = \overline{x}_i(0)$ be its corresponding points of X. By universal property of the fiber product, we have a morphism $\overline{x} : Spec(k) \to X^n$, where $X^n = X \times_S ... \times_s X$ (n-times), such that $p_i \circ \overline{x} = \overline{x}_i$, where $p_i : X^n \to X$ is the canonical i-th projection. Let P be the connected component of X^n such that the image of $\overline{x}$ is contained in P. Consider the inclusion morphism $i : P \to X$, then the morphism $\psi := p_1 \circ i : P \to X$ is finite étale (since p_1 is a change of base of a finite étale morphism).
P is a Galois covering of X: Indeed, for every $i, j \in \{1, ..., n\}$ consider the proyection $p_{i,j} : X^n \to X \times_S X$ in the i-th and j-th coordinate. As $\varphi : X \to S$ is finite étale, then we have that the diagonal morphisms $\Delta : X \to X \times_S X$ is open and closed. If $P \cap p_{i,j}^{-1}(\Delta(X)) \neq \emptyset$, then by the connectedness of P, we have that $P \subseteq p_{i,j}^{-1}(\Delta(X))$ (otherwise $P \cap p_{i,j}^{-1}(\Delta(X))$ and $P \cap (p_{i,j}^{-1}(\Delta(X)))^c$ is a disconnection of P), this is a contradiction, since $x \in P \setminus p_{i,j}^{-1}(\Delta(X))$ (the i-th and j-th coordinates of x are different). Thus $P \cap \pi_{i,j}^{-1}(\Delta(X)) = \emptyset$ therefore for every $i, j \in \{1, ..., n\}$. Thus all the points in P have different coordinates.
Note that

$$\begin{aligned} X_{\overline{s}}^n &= X^n \times_S Spec(k) \\ &= X \times_S ... \times_S X \times_S Spec(k) \\ &= X \times_S Spec(k) \times_S .... \times_S X \times_S Spec(k) \\ &= X_{\overline{s}} \times_S ... \times_S X_{\overline{s}}, \end{aligned}$$

and therefore $P_{\overline{s}}$ is a subset of $\{\overline{x}_1, ..., \overline{x}_n\}^n$, but we prove that the points in P have different coordinates, therefore there exists a subgroup A of the group S_n of the permutations in n-words, such that

$$P_{\overline{s}} = \{(x_{\sigma(1)}, ..., x_{\sigma(n)}) \in X^n | \sigma \in A\}.$$

An element $\sigma \in A$, induces an automorphism $\hat{\sigma} : X^n \to X^n$, such that $\hat{\sigma}((\overline{x}_i)) = (\overline{x}_{\sigma(i)})$ (induced by the identity morphism $X \to X$ where the left X corresponds to the i-th element of the product X^n and the right X corresponds to the $\sigma(i)$-th element of the product X^n). Furthermore, $\hat{\sigma}$ restricts to an automorphism of P, since $\hat{\sigma}(\overline{x}) \in P$ (see the description of the geometric fiber $P_{\overline{s}}$), and $\hat{\sigma}(P)$, P are component connected components containing $\overline{x}$, then $\hat{\sigma}(P) = P$. Thus, the element $\hat{\sigma}|_P \in Aut(P|S)$ send the geometric point $(\overline{x}_i)$ in the geometric point $(\overline{x}_{\sigma(i)})$, since A is a subgroup of S_n, this implies that $Aut(P|S)$ acts transitively in one geometric fiber and therefore, P is a Galois covering of S.
It remains to prove the universal property, let $\phi : Z \to X$, be a connected finite étale covering of X, such that $\psi \circ \phi : Z \to S$ is a Galois covering. Let $\overline{z} \in Z_{\overline{x}}$, note that $\overline{z} \in Z_{\overline{s}}$, since Z is a Galois covering of S, there exists automorphisms $p_i \in Aut(Z|S)$, such that $\phi \circ p_i(\overline{z}) = \overline{x}_i$. The universal property of the fiber product implies that there exists a unique morphism $\alpha : Z \to X^n$, such that $p_i \circ \alpha = \phi \circ p_i$. In particular we know that $\overline{x} \in \alpha(Z)$ and since Z is connected, this implies that $Z \subseteq P$, therefore φ factors through α and ψ □

Before we state one of the principal theorems about Galois coverings, we have to study quotients by certain group actions. Let X be an S-scheme and G be a subgroup of $Aut(X|S)$. G acts on X if we define the next action

$$\begin{aligned} G \times X &\to X \\ (\sigma, x) &\mapsto \sigma(x), \end{aligned}$$

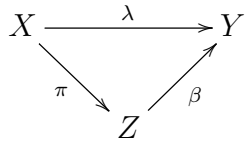
at level of topological spaces, we know what it means the quotient of X by G. But, what it means the quotient of a scheme by a group action? The next definition is a categorical view of this question, but next to this definition we give an idea of how to construct this quotients.

Definition 3.3.8. *Let $f : X \to S$ be an affine morphism of schemes and G is a subgroups of $Aut(X|S)$. A morphism $\pi : X \to Z$ is called the* ***quotient*** *of X by G, if*

(i) π is affine and surjective.

(ii) π is constant in orbits, i.e., if $x, y \in X$, satisfies that $Orb_x = Orb_y$, then $\pi(x) = \pi(y)$.

(iii) If $\lambda : X \to Y$ is an affine, surjective and constant in orbits morphism, then there exists a unique morphism $\beta : Z \to Y$, such that the next diagram is commutative



in this case we denote Z by X/G.

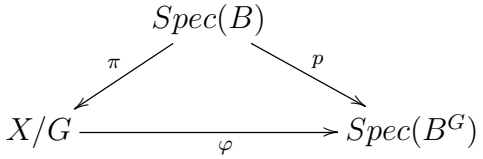
Proposition 3.3.7. *If $\varphi : X \to S$ is an affine, surjective morphism and G is a subgroup of $Aut(X|S)$, then exists a quotient of X by G.*

We give an sketch of this prove, the idea is to construct a locally ringed space X/G and a morphism of locally ringed spaces $\pi : X \to X/G$, then prove that X/G is an scheme. The underlying topological space of X/G is the topological quotient of the space of X by the action of G. The sheaf $\mathcal{O}_{X/G}$ is defined in every open subset U of X, by

$$\begin{aligned} \mathcal{O}_{X/G}(U) &= \pi^*(\mathcal{O}_X)(U)^G \\ &= \{g \in \pi^*(\mathcal{O}_X)(U) | \sigma(g) = g, for \ \ every \ \ \sigma \in G\}, \end{aligned}$$

where $\pi^*(\mathcal{O}_X)$, denotes the pullback via π.

We want to prove that $(X/G, \mathcal{O}_{X/G})$ is a scheme. We can reduce it to the affine case, i.e., where $X = Spec(B)$, $S = Spec(A)$ and φ is induced by a ring homomorphim $f : A \to B$. Let B^G be the subring of B of G-invariants, the inclusion map $B \to B^G$, produces a scheme morphism $p : Spec(B) \to Spec(B^G)$, using that B^G is integral over B, we can prove that p is surjective. Now, the idea is construct an isomorphism of locally ringed spaces $\psi : X/G \to Spec(B^G)$, such that the next diagram is commutative



and this prove that X/G is an affine scheme. For every $x \in Spec(B)$, we define $\varphi([x]) = p(x)$, where $[x]$ denotes the class of x in X/G, this is a well-defined isomorphism as a consequence of the chinese remainder theorem. And finally to prove isomorphism of the associated sheaves, consider the next morphism of sheaves

$$\begin{aligned} \phi : \pi_*\mathcal{O}_X &\to \bigoplus_{\sigma \in G} \pi_*\mathcal{O}_X \\ s &\mapsto (\sigma(s) - s)_{\sigma \in G}, \end{aligned}$$

then $ker(\varphi) = \mathcal{O}_{X/G}$, in particular, $\mathcal{O}_{X/G}$ if a quasi-coherent sheaf, therefore it is sufficent to prove that the global sections of $\mathcal{O}_{X/G}$ and $\mathcal{O}_{Spec(B^G)}$ are isomorphic rings, which is trivial. This completes the proof.

Proposition 3.3.8. *Let $\varphi : X \to S$ be a connected étale finite cover of S. If G is a subgroup of $Aut(X|S)$, then $\pi : X \to X/G$ is a finite étale cover of X/G and the induced morphism $\psi : X/G \to S$ is a finite étale cover of S.*

Proof. Note that φ is in particular an affine surjective morphism, then there exists the quotien $\pi : X \to X/G$. We first prove that the induced morphism $\psi : X \to S$ is a finite étale covering of S. By the local behaviour of finite étale coverings, there exists a locally free morphism $F : Y \to S$, such that

$$X \times_S Y \simeq F \times Y,$$

where F is a finite set. The action of G in X, can be extended to an action of G in $X \times_S Y$, if we define

$$\begin{aligned} G \times (X \times_S Y) &\to X \times_S Y \\ (\sigma, y) &\mapsto f_\sigma(y), \end{aligned}$$

where $f_\sigma = \sigma \times id_Y$ (doing the base change of the automorphism $\sigma : X \to X$ by Y). This action, in particular, induces a natural action on F and we have the next isomorphism

$$(X \times_S Y)/G \simeq (F/G) \times_S Y.$$

Consider the natural morphism

$$X \times_S Y \to (X/G) \times_S Y,$$

this morphism is constant in G-orbits and therefore can be factorized in the quotient $(X \times_S Y)/G$. In other words, there exists a morphism

$$(X \times_S Y)/G \to (X/G) \times_S Y,$$

we want to show that this morphism is actually an isomorphism. We want to prove it locally and using cocycle conditions we can glue this isomorphism to check that the previous morphism is an isomorphism. Let $Spec(A)$ be an affine open subset of S sufficiently small such that $\varphi^{-1}(Spec(A)) = Spec(B)$ is an affine open subset of X, $F^{-1}(Spec(A)) = Spec(C)$ is an affine open subset of Y, with C a free A-module ($F : Y \to S$ is locally free). Then we have to prove that

$$B^G \bigotimes_A C \simeq (B \otimes_A C)^G,$$

this is trivially true because the action on Y is trivial. Therefore,

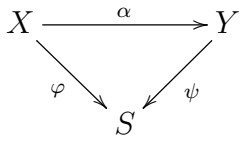
$$\begin{aligned} (X \times_S Y)/G &\simeq (X/G) \times Y \\ &\simeq (F/G) \times Y, \end{aligned}$$

and therefore, $(X \times_S Y)/G$ is a finite étale covering, using again the local behaviour of the étale morphisms.
Using that the next diagram is commutative

$$\begin{array}{ccc} X & \xrightarrow{\pi} & X/G \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\psi} & \\ & S & \end{array}$$

and that φ, ψ are finite étale coverings, then the same is true for π. □

Let $\varphi : X \to S$ be a Galois covering of S, we denote by $F\acute{E}t_S^X$ the set of classes of S-isomorphisms of finite étale coverings $\psi : Y \to S$ of S, such that there exists a finite étale morphism $\alpha : X \to Y$, such that, the next diagram is commutative



Theorem 3.3.3. *Let $\varphi : X \to Y$ be a Galois covering. The function*

$$\begin{aligned} G : F\acute{E}t_S^X &\to Sub(Aut(X|S)) \\ [Y] &\mapsto Aut(X|Y), \end{aligned}$$

is a bijection, where $Sub(Aut(X|S))$ is the set of subgroups of $Aut(X|S)$. The inverse function of G is

$$\begin{aligned} F : Sub(Aut(X|S)) &\to F\acute{E}t_S^X \\ H &\mapsto [X/H]. \end{aligned}$$

Moreover, we have that an element $[Y] \in F\acute{E}t_S^X$ is represented by a Galois covering $Y \to S$ if, and only if, $Aut(X|Y)$ is a normal subgroup of $Aut(X|S)$.

3.4 Étale fundamental group

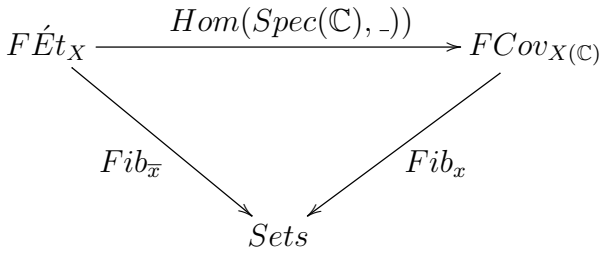
In this section we introduce and discuss some examples of the étale fundamental group, we explore the Grothendieck's main theorem of étale fundamental group theory and we see some consequences in field theory. With the idea that finite é covers of a scheme are like the covering spaces of a topological space, it is clear how to construct a correct analogue to the fundamental group.
Let X be a scheme and $\overline{x} : Spec(k) \to X$ be a geometric point and x the associated point of x in X. The *fiber functor* of X at $\overline{x}$ is defined to be

$$\begin{aligned} Fib_{\overline{x}} : F\acute{E}t_X &\to Sets \\ (\varphi : Y \to X) &\mapsto \varphi^{-1}(x) \end{aligned}$$

As we mentioned before, as a set $\varphi^{-1}(X)$ is the same as $Y \times_X Spec(k)$, in some cases we use the functor $Fib_{\overline{x}}$ in the form of geometric fibers, instead as a usual set-theoretic fibers.

Definition 3.4.1. *Let X be a scheme and $\overline{x} : Spec(k) \to X$ be a geometric point. The **étale fundamental group** of X at $\overline{x}$, denoted by $\pi_1(X, \overline{x})$, is the group of natural automorphisms of $Fib_{\overline{x}}$.*

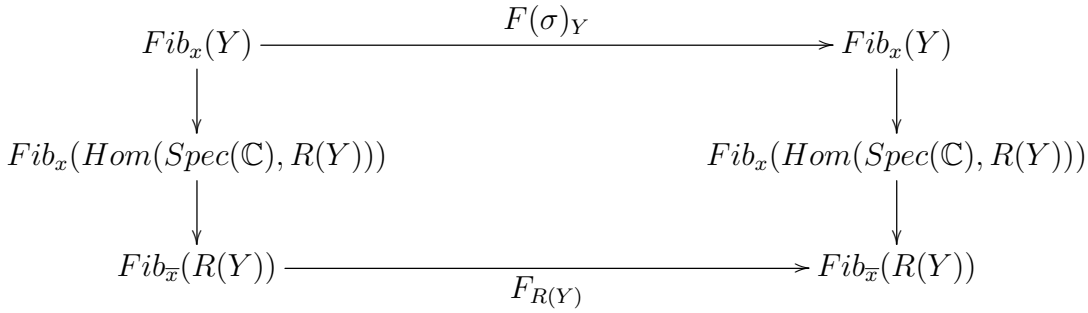
The definition of the étale fundamental group, is not too good for make computations: it is necessary to classify all the finite étale coverings of a scheme and then compute the group of natural isomorphisms of the fiber functor.
Let X be a complex variety and $\overline{x} : Spec(\mathbb{C}) \to X$ be a geometric point and x be the associated point in X. Consider the next commutative diagram



where Fib_x is the topological fiber functor as is defined in the first section of this chapter. By Grothendieck-Riemann generalized existence theorem we have that $Hom(Spec(\mathbb{C}), \_)$ is an equivalence of categories, denote by R be its dual functor. The function

$$\begin{aligned} G : \pi_1(X, \overline{x}) &\to Aut(Fib_x) \\ \sigma &\to F(\sigma) \end{aligned}$$

such that, $F(\sigma)$ is the natural automorphism of the functor Fib_X defined in every finite covering space $f : Y \to X(\mathbb{C})$, in the next diagram, where the vertical arrows are the isomorphisms associated to the equivalence R



Crearly, under this definition G is a biyection. But, as we see in the section one of this chapter, $Aut(Fib_x)$ is the profinite completion of the fundamental group $\pi_1(X(\mathbb{C}), x)$. For a group G, we denote by $\widehat{G}$ the profinite completion of G. We have the next beautiful connection between the étale fundamental group and the usual fundamental group in the complex-case.

Theorem 3.4.1. *If X is a complex variety, then $\pi_1^{\acute{e}t}(X, \overline{x}) \simeq \pi_1(\widehat{X(\mathbb{C})}, x)$.*

In the next three examples $\overline{x}$ is a $\mathbb{C}$-rational point (in particular a geometric point). Using the previous theorem we have that

(i) $\pi_1^{\acute{e}t}(\mathbb{A}^1_{\mathbb{C},\overline{x}}) = 0$,

(ii) $\pi_1^{\acute{e}t}(\mathbb{A}^1_{\mathbb{C}} \setminus \{0\}, \overline{x}) = \widehat{\mathbb{Z}}$,

(iii) $\pi_1^{\acute{e}t}(\mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\}, \overline{x}) = \widehat{F(x,y)}$, where $F(x,y)$ is the free group in the two generators x and y.

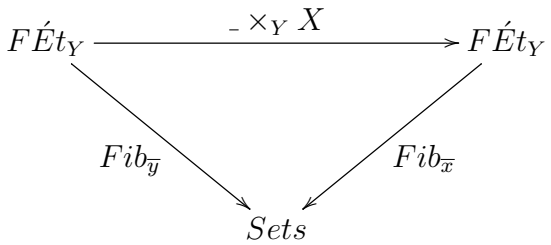
The first example return us the intuitive idea of that $\mathbb{A}^1_{\mathbb{C}}$ is a simply connected space. Another example, but this time coming from arithmetic is the computation of $\pi_1^{\acute{e}t}(Spec(\mathbb{Z}, \overline{x})$, for some geometric point $\overline{x}$ of $Spec(\mathbb{Z})$. A finite étale covering $\varphi : Y \to Spec(Z)$, the surjectivity of φ implies that there exists $y \in Y$ such that $\varphi(y) = 0$, the generic point of $Spec(\mathbb{Z})$ since φ is étale, in particular, is étale at y, then we can produce a finite unramified extension field on the rational numbers (unramified in the sense of algebraic number theory), but this is not posible since the absolute value of the discriminant of every number field k (other than $\mathbb{Q}$ itself) is greater than 1 and therefore a prime number divides it, this prime number ramifies in k (see [24] for details). Thus, the category of finite étale coverings of $Spec(\mathbb{Z})$ is reduced to one object $Spec(\mathbb{Z})$ itself. And thus, the $\pi_1^{\acute{e}t}(Spec(\mathbb{Z})) = 0$

Definition 3.4.2. *Let X be a connected scheme. We say that X is **simply connected** if $\pi_1^{\acute{e}t}(X, \overline{x})$ is the trivial group.*

If $\varphi : X \to Y$ is a morphism and $\overline{x} : Spec(k) \to X$ is a geometric point of X, then $\overline{y} := \varphi(\overline{x}) : Spec(k) \to Y$ is a geometric point of Y. Consider the change of base functor

$$\begin{aligned} \_ \times_Y X : F\acute{E}t_Y &\to F\acute{E}t_X \\ Z &\mapsto Z \times_Y X, \end{aligned}$$

then the next diagram is commutative



indeed, if Z is an object of $F\acute{E}t_Y$, then

$$\begin{aligned} Fib_{\overline{x}} \circ (\_ \times_Y X)(Z) &= Fib_{\overline{x}}(Z \times_Y X) \\ &= Z \times_Y X \times_X Spec(k) \\ &= Z \times_Y Spec(k) \\ &= Fib_{\overline{y}}(Z). \end{aligned}$$

Therefore, for every $\sigma \in \pi_1^{ét}(X, \overline{x})$, we can define

$$F(\sigma) : Fib_{\overline{y}} \rightarrow Fib_{\overline{y}}$$

such that $F(\sigma)_Z = \sigma_{Z\times_Y X}$, for every object Z of $F\acute{E}t_Y$. $F(\sigma) \in \pi_1^{ét}(Y, \overline{y})$ (it is a natural automorphism of $Fib_{\overline{y}}$ with inverse $F(\sigma^{-1})$), and therefore we define a function

$$\begin{aligned} \pi_1^{ét}(\varphi) : \pi_1^{ét}(X, \overline{x}) &\rightarrow \pi_1^{ét}(Y, \overline{y}) \\ \sigma &\mapsto F(\sigma), \end{aligned}$$

moreover, $\pi^{ét}(\varphi)$ is a group homomorphism , indeed for $\sigma, \theta \in \pi_1^{ét}(X, \overline{x})$,

$$\begin{aligned} F(\sigma \circ \theta)_Z &= (\sigma \circ \theta)_{Z\times_Y X} \\ &= \sigma_{Z\times_Y X} \circ \theta_{Z\times_Y X} \\ &= F(\sigma)_Z \circ F(\sigma)_Z. \end{aligned}$$

Let X be a scheme. We say that $(X, \overline{x})$ is a pointed scheme with a k-valued point if k is an algebraically closed field and $\overline{x} : Spec(k) \rightarrow X$ is a geometric point of X. A morphism of a pointed schemes $\varphi : (X, \overline{x}) \rightarrow (Y, \overline{y})$ is a morphism of schemes $\varphi : X \rightarrow Y$, such that $\varphi(\overline{x}) = \overline{y}$. Let Sch^k be the category of pointed schemes with a k-valued point. Moreover, we have that.

Theorem 3.4.2.

$$\begin{aligned} \pi_1^{ét} : Sch^k &\rightarrow Grp \\ (X, \overline{x}) &\mapsto \pi_1^{ét}(X, \overline{x}), \end{aligned}$$

is a (covariant) functor, where Grp is the category of groups.

We saw in the section 1 of this chapter under some hypothesis over a topological space X, the (topological) fiber functor Fib_x, for a point $x \in X$, is representable, i.e., there exists a covering space $\widetilde{X} \rightarrow X$, we have a natural isomorphism $Fib_x \simeq Hom(\widetilde{X}, \_)$, and moreover, we know that $\widetilde{X}$ is the universal covering space. In the section 2 of this chapter, we see how the existence of universal finite étale covering may fail with an example, therefore we dont have faith in that the (étale) fiber functor $Fib_{\overline{x}}$ be a representable functor. But, there is a similar property in the étale case?

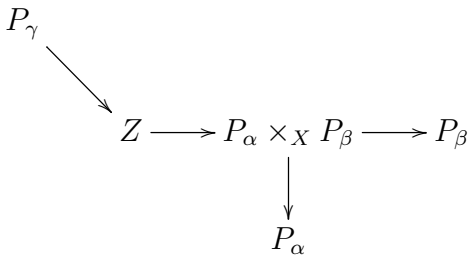
Definition 3.4.3. *Let $F : \mathfrak{C} \rightarrow Set$ be a funtor. We say that F is prorepresentable is there exists an inverse system $(P_\alpha, \phi_{\alpha,\beta})$ of objects in $\mathfrak{C}$, such that the next two functors are naturally isormorphic $\varinjlim Hom(P_\alpha, \_) \simeq F$.*

In the category of *Sets* we have the next characterization of limits. Let $(X_i, f_{ij})_{i,j\in I}$ be a directed system of sets, then the directed limit is a quotient of the disjoint union, $\bigsqcup_{i\in I} X_i$, where $x \in X_i$ is identified with $y \in X_j$ if, and only if there exists $k \in I$, with $k \geq i, j$, such that $f_{k,i}(x) = f_{k,j}(y)$.

Proposition 3.4.1. *If X is a connected scheme and $\overline{x} : Spec(k) \to X$ is a geometric point of X, then the functor $Fib_{\overline{x}} : F\acute{E}t : X \to Sets$ is prorepresentable.*

Proof. Let Λ be the set of Galois coverings of X. For every $P_\alpha \in \Lambda$ we fix a point $p_\alpha \in Fib_{\overline{x}}(P_\alpha)$. With this fixed points in every element of Λ, we can define the next order for $P_\alpha, P_\beta \in \Lambda$, we say that $P_\alpha \leq P_\beta$ if there exists a X-morphism $\phi_{\alpha,\beta} : P_\beta \to P_\alpha$, such that $\phi_{\alpha,\beta}(p_\beta) = p_\alpha$. Notice that if $P_\alpha \leq P_\beta$, then there exists a unique X-morphism $\phi_{\alpha,\beta} : P_\beta \to P_\alpha$, such that $\phi_{\alpha,\beta}(p_\beta) = p_\alpha$, indeed, if $\varphi : P_{\beta\alpha}$ is a X-morphism such that $\varphi(p_\beta) = p_\alpha$, then we have that $\varphi(p_\beta) = \phi_{\alpha,\beta}(p_\alpha)$. Let l be the residual field of p_β, taking and algebraic closure $\bar{l}$ of l, the inclusion map $l \hookrightarrow \bar{l}$ (after composing with an appropriate X-morphism of schemes $Spec(l) \to P_\beta$) induces a geometric point $\overline{p_\beta} : Spec(\bar{l}) \to P_\beta$, with associated point p_β. Moreover we have that $\varphi(\overline{p_\beta}) = \phi_{\alpha,\beta}(\overline{p_\beta})$, and therefore we have that $\varphi = \phi_{\alpha,\beta}$, by Proposition 3.3.3. In the rest of this proof, we denote by $\pi_{\alpha,\beta}$ this morphism, when exists.

There is an equivalent way to understand the same order in Λ: $P_\alpha \leq P_\beta$ if and only if there exists a X-morphism $\phi : P_\beta \to P_\alpha$, One direction of the previous equivalence is trivial. For the other one, let $\phi : P_\beta \to P_\alpha$ be a X-morphism. Note that ϕ is surjective (P_α, P_β are Galois coverings of X), let $c \in \phi^{-1}(p_\alpha)$, since ϕ is a X morphism, we have that $c \in Fib_{\overline{x}}(P_\beta)$. Then we have two points p_β, c in the fiber $Fib_{\overline{x}}(P_\beta)$ and P_β is a Galois covering of X, therefore the action of $Aut(P_\beta|X)$ in $Fib_{\overline{x}}(P_\beta)$ is transitive, thus there (a unique) exists $\sigma \in Aut(P_\beta|X)$ such that $\sigma(p_\beta) = c$, let $\varphi_{\alpha,\beta} = \phi \circ \sigma$, then $\varphi : P_\beta \to P_\alpha$ is a X-morphism, such that $\varphi(p_\beta) = p_\alpha$, this by definition is that $P_\alpha \leq P_\beta$.
Let $P_\alpha, P_\beta \in \Lambda$, then $P_\alpha \times_X P_\beta$ is a finite étale covering of X. Let Z be a connected component of $P_\alpha \times_X P_\beta$, Z is a finite étale covering of X too. By Proposition 3.3.6 it is possible to find a Galois closure of Z, equivalently, it is possible to find $P_\gamma \in \Lambda$, with an X-morphism $P_\Gamma \to Z$, therefore we have the next diagram of X-schemes



in particular, we have X-morphisms $P_\gamma \to P_\alpha$ and $P_\gamma \to P_\beta$, equivalently as we saw, $P_\alpha \leq P_\gamma$ and $P_\beta \leq P_\gamma$, therefore there exists a unique X-morphisms $\phi_{\alpha,\gamma} : P_\gamma \to P_\alpha$ and $\phi_{\beta,\gamma} : P_\gamma \to P_\beta$, such that $\phi_{\alpha,\gamma}(p_\gamma) = p_\alpha$ and $\phi_{\beta,\gamma}(p_\gamma) = p_\beta$. Thus, $(P_\alpha, \phi_{\alpha,\beta})$ is a inverse system of objects in $F\acute{E}t_X$.

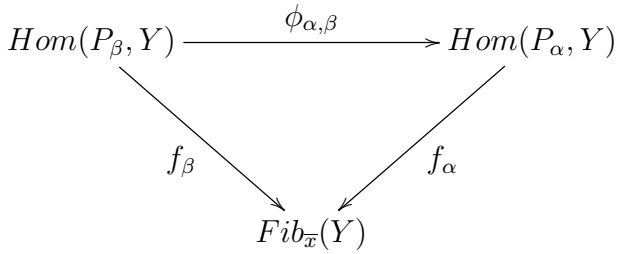
For every $P_\alpha \in \Lambda$ and every finite étale cover Y of X, let

$$\begin{aligned} f_\alpha : Hom(P_\alpha, Y) &\to Fib_{\overline{x}}(Y) \\ \varphi &\mapsto Fib_{\overline{x}}(\varphi)(p_\alpha). \end{aligned}$$

If $P_\beta \in \Lambda$, such that $P_\alpha \leq P_\beta$, we have a function

$$\begin{aligned} \widetilde{\phi_{\alpha,\beta}} : Hom(P_\beta, Y) &\to Hom(P_\alpha, Y) \\ \varphi &\mapsto \varphi \circ \phi_{\alpha,\beta}, \end{aligned}$$

and the next diagram is commutative



Indeed if $\varphi \in Hom(P_\beta, Y)$, then

$$\begin{aligned} f_\alpha \circ \widetilde{\phi_{\alpha,\beta}}(\varphi) &= f_\alpha(\varphi \circ \phi_{\alpha,\beta}) \\ &= Fib_{\overline{x}}(\varphi \circ \phi_{\alpha,\beta})(p_\alpha) \\ &= Fib_{\overline{x}}(\varphi) \circ Fib_{\overline{x}}(\phi_{\alpha,\beta})(p_\alpha) \\ &= Fib_{\overline{x}}(\varphi)(Fib_{\overline{x}}(\phi_{\alpha,\beta})(p_\alpha)) \\ &= Fib_{\overline{x}}(\varphi)(p_\beta) \\ &= f_\beta(\varphi) \end{aligned}$$

Thus, the function f_α, induces a function $f_Y : \varinjlim_{P_\alpha \in \lambda} Hom(P_\alpha, Y) \to Fib_{\overline{x}}(Y)$, for every finite étale cover Y of X. Explicitly,

$$\begin{aligned} f_Y : \varinjlim_{P_\alpha \in \lambda} Hom(P_\alpha, Y) &\to Fib_{\overline{x}}(Y) \\ [\varphi] &\mapsto f_\alpha(\varphi), \ if \ \varphi \in Hom(P_\alpha, Y) \end{aligned}$$

this is a well defined function and moreover $f = \{f_Y | Y \in Obj(F\acute{E}t_x)\}$ is a natural transformation. Furthermore f is a natural isomorphism, only we have to construct an inverse function g_Y of f_Y, for every finite étale cover of X. Without lose of generality we can suppose that Y is a connected scheme (otherwise take the connected components of Y). Let $y \in Y$, then by Proposition 3.3.6, there exists a Galois closure $f : P_\gamma \to Y$ of Y, in particular $P_\gamma \in \Lambda$, let $c \in f^{-1}(y)$. Using the fact that P_γ is Galois over X and that $c, p_\gamma \in Fib_{\overline{x}}(P_\gamma)$,

there exists a (unique) automorphism $\sigma \in Aut(P_\gamma|X)$, such that $\sigma(p_\beta) = c$, therefore we have that the X-morphism $F = f \circ \sigma : P_\gamma \to Y$, satisfies that $F(p_\beta) = y$. Define

$$\begin{aligned} g_Y : Fib_{\overline{x}}(Y) &\to \varinjlim_{P_\alpha \in \lambda} Hom(P_\alpha, Y) \\ y &\mapsto [F] \end{aligned}$$

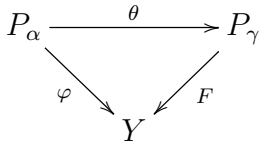
as constructed below. We want to prove that f_Y and g_Y are inverse one of each other. Indeed, let $y \in Fib_{\overline{x}}(Y)$,

$$\begin{aligned} f_Y \circ g_Y(y) &= f_Y(g_Y(y)) \\ &= f_Y([F]) \\ &= f_Y([f \circ \sigma]) \\ &= f_\gamma(f \circ \sigma) \\ &= Fib_{\overline{x}}(f \circ \sigma)(p_\gamma) \\ &= y \end{aligned}$$

as we seen before. If $[\varphi] \in \varinjlim_{P_\alpha \in \lambda} Hom(P_\alpha, Y)$, with $\varphi \in Hom(P_\alpha, Y)$, then

$$\begin{aligned} g_Y \circ f_Y([\varphi]) &= g_Y(f_Y([\varphi])) \\ &= g_Y(f_\alpha(\varphi)) \\ &= g_Y(Fib_{\overline{x}}(\varphi)(p_\alpha)) \\ &= [F] \end{aligned}$$

where $F : P_\gamma \to Y$, is a X-morphism, such that $F(Fib_{\overline{x}}(\varphi)(p_\alpha)) = y$. Since $\varphi : P_\alpha \to Y$ is a X-morphism, then there exists a unique morphism $\theta : P_\alpha \to P_\gamma$, such that the next diagram is commutative



(P_γ is the Galois closure of Y). Since $F \circ \phi_{\gamma,\alpha}(p_\alpha) = y$, then we have $F \circ \phi_{\gamma,\alpha}(\overline{p_\alpha}) = \overline{y}$ for suitable geometric points of P_α and Y, respectively. Thus by Proposition 3.3.3, we have that $F \circ \phi_{\gamma,\alpha} = \varphi$, and by the uniqueness of θ we have that $\theta = \phi_{\gamma,\alpha}$. Equivalentely, via the function

$$\widetilde{\phi_{\gamma,\alpha}} : Hom(P_\gamma, Y) \to Hom(P_\alpha, Y),$$

we have that $\widetilde{\phi_{\gamma,\alpha}}(F) = \varphi = \widetilde{\alpha,\alpha}(\varphi)$, this means, in particular that $[F] = [\varphi]$, and therefore $g_Y \circ f_Y([\varphi]) = [\varphi]$. Finally, we conclude that f is a natural biyection and therefore $Fib_{\overline{x}}$ is a pro-representable functor. □

Definition 3.4.4. *Let $(P_\alpha, \phi_{\alpha,\beta})_{\alpha,\beta\in\Lambda}$ be a inverse system of objects in a category $\mathfrak{C}$. An **automorphism** of this system is a collection of automorphisms $\phi_\alpha : P_\alpha \to P_\alpha$ for each $\alpha \in \Lambda$, such that for every $\alpha, \beta \in \Lambda$ with $\alpha \leq \beta$, the next diagram is commutative*

$$\begin{array}{ccc} P_\beta & \xrightarrow{\phi_{\alpha,\beta}} & P_\alpha \\ {\scriptstyle\phi_\beta}\downarrow & & \downarrow{\scriptstyle\phi_\alpha} \\ P_\beta & \xrightarrow[\phi_{\alpha,\beta}]{} & P_\alpha \end{array}$$

we denote by $(\phi_\alpha)_{\alpha\in\Lambda}$ (or simply (ϕ_α), when Λ) is clear) to such automorphism.

For a inverse system of objects $(P_\alpha, \phi_{\alpha,\beta})$, we denote by $Aut(P_\alpha, \phi_{\alpha,\beta})$ the set of automorphisms of this inverse system. $Aut(P_\alpha, \phi_{\alpha,\beta})$ is a group under compostion, i. e., is a group with the operation $(\phi_\alpha) \circ (\phi_\beta) = (\phi_\alpha \circ \phi_\beta)$.
Let X be a connected scheme and $\overline{x}$ be a geometric point of X. In the rest of this section we use the notation and conventions of the proof in the previous proposition. If (ϕ_α) is an automorphism of $(P_\alpha, \phi_{\alpha,\beta})$, then it is clear that the asociated bijections $\widetilde{\phi_\alpha} : Hom(P_\alpha, X) \to Hom(P_\alpha, X)$, are compatible with $\widetilde{\phi_{\alpha,\beta}}$. Therefore, $\widetilde{\phi_\alpha}$ induces a bijection

$$\varinjlim_{P_\alpha\in\lambda} \phi_\alpha : \varinjlim_{P_\alpha\in\lambda} Hom(P_\alpha, Y) \to \varinjlim_{P_\alpha\in\lambda} Hom(P_\alpha, Y),$$

for every finite étale cover Y of X, which is characterized for $\varphi \in Hom(P_\alpha, X)$, by $\varinjlim_{P_\alpha\in\lambda} \phi_\alpha([\varphi]) = [\varphi \circ \phi_\alpha]$.

Proposition 3.4.2. *If X is a connected scheme and $\overline{x}$ is a geometric point of X, the function*

$$\begin{array}{rcl} F : Aut(P_\alpha, \phi_{\alpha,\beta}) & \to & \pi_1^{\acute{e}t}(X, \overline{x}) \\ (\phi_\alpha) & \mapsto & f \circ \varinjlim_{\alpha\in\lambda} \widetilde{\phi_\alpha} \circ f^{-1} \end{array}$$

is bijective. Where,

$$f : \varinjlim_{P_\alpha\in\lambda} Hom(P_\alpha, \_) \to Fib_{\overline{x}}$$

is the natural isomorphism described in the proof of the previous proposition.

Proof. First, we prove that F is surjective.
For every $P_\alpha \in \Lambda$, we have an automorphism

$$\sigma_{P_\alpha} : Fib_{\overline{x}}(P_\alpha) \to Fib_{\overline{x}}(P_\alpha),$$

for every α, let $q_\alpha = \sigma_{P_\alpha}(p_\alpha)$. Since P_α is a Galois covering of X, then there exists (a unique) $\phi_\alpha \in Aut(P_\alpha|X)$, such that $\phi_\alpha(p_\alpha) = q_\alpha$. First, we want to prove that (ϕ_α) is an automorphism of the inverse system $(P_\alpha, \phi_{\alpha,\beta})$. Since σ is a natural automorphism of $Fib_{\overline{x}}$, then we know that the next diagram is commutative

$$\begin{array}{ccc} Fib_{\overline{x}}(P_\alpha) & \xrightarrow{\sigma_{P_\alpha}} & Fib_{\overline{x}}(P_\alpha) \\ \downarrow{\scriptstyle Fib_{\overline{x}}(\phi_{\alpha,\beta})} & & \downarrow{\scriptstyle Fib_{\overline{x}}(\phi_{\alpha,\beta})} \\ Fib_{\overline{x}}(P_\beta) & \xrightarrow[\sigma_{P_\beta}]{} & Fib_{\overline{x}}(P_\beta) \end{array}$$

In particular, we know that

$$\begin{aligned} Fib_{\overline{x}}(\phi_{\alpha,\beta})(q_\alpha) &= Fib_{\overline{x}}(\phi_{\alpha,\beta})(\sigma_{P_\alpha}(p_\alpha)) \\ &= \sigma_{P_\beta}(p_\beta) \\ &= q_\beta, \end{aligned}$$

Therefore, we have that $\phi_{\alpha,\beta}(q_\alpha) = q_\beta$, or equivalently, that $\phi_\beta \circ \phi_{\alpha,\beta}(p_\alpha) = \phi_{\alpha,\beta} \circ \phi_\alpha(p_\alpha)$ and after taking a suitable geometric point of P_α, we can conclude that $\phi_\beta \circ \phi_{\alpha,\beta} = \phi_{\alpha,\beta} \circ \phi_\alpha$, using Proposition 3.3.3. Then (ϕ_α) is an automorphism of $(P_\alpha, \phi_{\alpha,\beta})$.
Let Y be a finite étale covering of X, we have to prove that

$$f_Y \circ \varinjlim_{\alpha\in\lambda} \phi_\alpha \circ f_Y^{-1} = \sigma_Y,$$

or equivalently that

$$f_Y \circ \varinjlim_{P_\alpha\in\lambda} \phi_\alpha = \sigma_Y \circ f_Y$$

Let $\varphi \in Hom(P_\alpha, Y)$, then considering the commutative diagram

$$\begin{array}{ccc} P_\alpha & \xrightarrow{\sigma_{P_\alpha}} & P_\alpha \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ Y & \xrightarrow[\sigma_Y]{} & Y \end{array}$$

we have that, $\varphi \circ \sigma_{p_\alpha}(p_\alpha) = \sigma_y \circ \varphi(p_\alpha)$, equivalently, $f_Y \circ \phi_\alpha(\varphi) = \sigma_Y \circ f_Y(\varphi)$, then the assertion follows.

□

Unfortunately, the function F described in the previous corollary is not an isomorphism of groups. Indeed if $(\phi_\alpha), (\lambda_\alpha) \in Aut(P_\alpha, \phi_{\alpha,\beta})$, then

$$\begin{aligned} F(\phi_\alpha \circ \lambda_\alpha) &= f \circ \varinjlim_{\alpha\in\lambda} \widetilde{\phi_\alpha \circ \lambda_\alpha} \circ f^{-1} \\ &= f \circ \varinjlim_{\alpha\in\lambda} \widetilde{\lambda_\alpha} \circ \widetilde{\phi_\alpha} \circ f^{-1} \\ &= f \circ \varinjlim_{\alpha\in\lambda} \widetilde{\lambda_\alpha} \circ \varinjlim_{\alpha\in\lambda} \widetilde{\phi_\alpha} \circ f^{-1} \\ &= f \circ \varinjlim_{\alpha\in\lambda} \widetilde{\lambda_\alpha} \circ f^{-1} \circ f \circ \varinjlim_{\alpha\in\lambda} \widetilde{\phi_\alpha} \circ f^{-1} \\ &= F(\lambda_\alpha) \circ F(\phi_\alpha) \end{aligned}$$

but, the previous computation show that if we take the opposite group $Aut(P_\alpha, \phi_{\alpha,\beta})^{op}$ (the same set but reversing the operation) of $Aut(P_\alpha, \phi_{\alpha,\beta})$, then we have the next isomorphism

$$\pi_1^{\acute{e}t}(X, \overline{x}) \simeq Aut(P_\alpha, \phi_{\alpha,\beta})^{op}$$

for every geometric point $\overline{x}$ of a connected scheme X. Note that this isomorphism not implies that the étale fundamental group dooes not depend on a geometric point $\overline{x}$, because the morphisms $\phi_{\alpha,\beta}$ depends on $\overline{x}$.
Now, if we study the group $Aut(P_\alpha, \phi_{\alpha,\beta})$, then we can see new properties of $\pi_1^{\acute{e}t}(X, \overline{x})$. For every $\beta \in \lambda$ let

$$\begin{aligned} F_\beta : Aut(P_\alpha, \phi_{\alpha,\beta}) &\to Aut(P_\beta|X) \\ (\phi_\alpha) &\mapsto \phi_\beta. \end{aligned}$$

F_β is surjective. Indeed, let $\phi_\beta \in Aut(P_\beta|X)$, for every $\alpha \in \Lambda$, there exists $\gamma \in \Lambda$ with $\alpha \leq \gamma$ and $\beta \leq \gamma$. In particular, we have the next X-morphisms $\phi_{\alpha,\gamma} : P_\gamma \to P_\alpha$ and $\phi_{\beta,\gamma} : P_\gamma \to P_\beta$. Let $q_\beta = \phi_{\beta,\gamma}(p_\beta)$ and $q_\gamma \in \phi^{-1}_{\beta,\gamma}(q_\beta)$, then $\phi_{\alpha,\gamma}(q_\gamma) \in Fib_{\overline{x}}(P_\alpha)$, taking a suitable geometric point and using that P_α is a Galois covering of X, there exists a unique automorphism $\phi_\alpha \in Aut(P_\alpha|X)$, such that $\phi_\alpha(p_\beta) = q_\alpha$. $(\phi_\alpha) \in Aut(P_\alpha, \phi_{\alpha,\beta})$, indeed, if $\beta_1, \beta_2 \in \Lambda$, such that $\beta_2 \leq \beta_1$, then there exists $\gamma \in \Lambda$, with $\beta_1, \beta_2, \beta \leq \gamma$, $\phi_{\beta_2,\gamma}(q_\gamma) = q_{\beta_2}$ and $\phi_{\beta_1,\gamma}(q_\gamma) = q_{\beta_1}$. Thus,

$$\begin{aligned} \phi_{\beta_1,\beta_2}(\phi_{\beta_2,\gamma}(q_\gamma)) = \phi_{\beta_1,\gamma}(q_\gamma) &\Leftrightarrow \phi_{\beta_1,\beta_2}(q_{\beta_2}) = q_{\beta_1} \\ &\Leftrightarrow \phi_{\beta_1,\beta_2}(\phi_{\beta_2}(p_{\beta_2})) = \phi_{\beta_1}(p_{\beta_1}) \\ &\Leftrightarrow \phi_{\beta_1}(\phi_{\beta_1,\beta_2}(p_{\beta_2})) \\ &\Leftrightarrow \phi_{\beta_1} \circ \phi_{\beta_1,\beta_2}(p_{\beta_2}) = \phi_{\beta_1,\beta_2} \circ \phi_{\beta_2}(p_{\beta_2})) \\ &\Leftrightarrow \phi_{\beta_1} \circ \phi_{\beta_1,\beta_2} = \phi_{\beta_1,\beta_2} \circ \phi_{\beta_2}, \end{aligned}$$

the last equivalence holds taking a suitable geometric point and using Proposition 3.3.3. Therefore, $(\phi_\alpha) \in Aut(P_\alpha, \phi_{\alpha,\beta})$ and trivially $F_\beta((\phi_\alpha)) = \phi_\beta$. Thus F_β is surjective, or equivalently, $Aut(P_\beta|X)$ is a quotient of $Aut(P_\alpha, \phi_{\alpha,\beta})$. Moreover, we have the next proposition.

Proposition 3.4.3. *If X is a connected scheme, then*

$$Aut(P_\alpha, \phi_{\alpha,\beta}) \simeq \varprojlim_{\alpha\in\lambda} Aut(P_\alpha|X).$$

Proof. Recall that in the category of groups $\varprojlim_{\alpha\in\lambda} Aut(P_\alpha|X)$ is a subgroup of the product group $\prod_{\alpha\in\Lambda} Aut(P_\alpha|X)$, we denote by $\prod g_\alpha$ an element of this product group. Let

$$\begin{aligned} F : Aut(P_\alpha, \phi_{\alpha,\beta}) &\to \varprojlim_{\alpha\in\lambda} Aut(P_\alpha|X) \\ (\phi_\alpha) &\mapsto \prod F_\alpha(\phi_\alpha) \end{aligned}$$

it is clear that F is an isomorphism. □

Corollary 3.4.1. *If X is a connected scheme and $\overline{x}$ is a geometric point of X, then $\pi^{ét}(X, \overline{x})$ is a profinite group.*

Proof.

$$\begin{aligned} \pi_1^{ét}(X, \overline{x}) &\simeq Aut(P_\alpha, \varphi_{\alpha,\beta})^{op} \\ &\simeq (\varprojlim_{\alpha\in\lambda} Aut(P_\alpha|X))^{op} \\ &\simeq \varprojlim_{\alpha\in\lambda} Aut(P_\alpha|X))^{op} \end{aligned}$$

since P_α is Galois covering, in particular, a finite Galois covering we know that $Aut(P_\alpha|X)^{op}$ is a finite group, this completes the proof. □

The last corollary and its prove allow us to reduce the computation of étale groups to computations of inverse limits of automorphisms of Galois coverings. For example, let k be a field, $X = Spec(k)$ and $\overline{x} : Spec(\overline{k}) \to Spec(k)$, the geometric point induced by the inclusion map $k \hookrightarrow \overline{k}$, where $\overline{k}$ is an algebraic closure of k. If $\varphi : Y \to Spec(k)$ is a Galois covering of $Spec(k)$, in particular, φ is finite étale and then $Y = Spec(A)$, where A is a finite étale k-algebra and φ is induced by the morphism $k \to A$. Therefore, there exists finite separable extensions $k_1, ..., k_n$ of k, such that

$$A \simeq k_1 \times ... \times k_n,$$

then we have that $Spec(A) = \bigsqcup_{i=1}^n Spec(k_i)$, but $Spec(A)$ is a Galois covering of $Spec(k)$, in particular, it is a connected scheme therefore $n = 1$. Reciprocally, if k_1 is a finite separable extension of k, then $Spec(k_1)$ is a Galois covering of $Spec(k)$. Thus the Galois coverings of the spectra of a field are spectra of a finite separable extensions of k. Moreover we have the next coequivalence of categories.

Theorem 3.4.3. *$Spec : FS_k \to Gal_{Spec(k)}$ is a coequivalence of categories, where FS_k is the category of finite separable extensions of k and $Gal_{Spec(k)}$ is the category of Galois coverings of k*

Then in the same situation of that $X = Spec(k)$ and $\overline{x} : Spec(\overline{k}) \to Spec(k)$, then there exists P_α Galois coverings of $Spec(k)$ such that

$$\pi_1^{\acute{e}t}(Spec(k), \overline{x}) \simeq \varprojlim_{\alpha\in\lambda} Aut(P_\alpha|Spec(k)))^{op}.$$

since P_α is a Galois covering of $Spec(k)$, then there exists finite separable extensions k_α of k, such that $P_\alpha = Spec(k_\alpha)$. Thus

$$\begin{aligned}\pi_1^{\acute{e}t}(Spec(k), \overline{x}) &\simeq \varprojlim_{\alpha\in\lambda} Aut(P_\alpha|Spec(k)))^{op} \\ &\simeq \varprojlim_{\alpha\in\lambda} Aut(Spec(k_\alpha)|Spec(k)))^{op} \\ &\simeq \varprojlim_{\alpha\in\lambda} Aut(k_\alpha|k),\end{aligned}$$

the last isomorphism is true using the coequivalence *Spec*. But $\varprojlim_{\alpha\in\lambda} Aut(k_\alpha|k)$ is isomorphic to $Gal(\overline{k}|k)$. Finally, we get the next beautiful isomorphism

$$\pi_1^{\acute{e}t}(Spec(k), \overline{k}) \simeq Gal(\overline{k}|k).$$

In one hand for spectra of a field the étale fundamental group is a incarnation of the absolute Galois group of this field, on the other hand for a complex algebraic variety the étale fundamental group is a incarnation of the profinite completion of the usual fundamental group of his complex points. In some sense, the étale fundamental group is a unifying both Galois groups and (topological) fundamental groups.

3.5 Grothendieck's geometrization of Galois theory

One of advantages of the definition of the étale fundamental group on scheme X (with a geometric point $\overline{x}$) is that $\pi_1^{\acute{e}t}(X, \overline{x})$ have an easy-to-define action on the (geometric) fibers of every finite étale cover. Indeed, if $\varphi : Y \to X$ is a finite étale morphism, then we can define the next action

$$\begin{aligned}\pi_1^{\acute{e}t}(X, \overline{x}) \times Fib_{\overline{x}}(Y) &\to Fib_{\overline{x}}(Y) \\ (\sigma, y) &\to Fib_{\overline{x}}(\sigma_Y)(y),\end{aligned}$$

(σ_Y is the automorphism of $Fib_{\overline{x}}(Y)$, associated to the natural transformation σ). In this section we study the behaviour of this actions, and connection with Galois theory.

Definition 3.5.1. *If $\varphi : Y \to X$ is a finite étale covering of X and $\overline{x}$ is a geometric point of X. The action of $\pi_1^{ét}(X, \overline{x})$ in $Fib_{\overline{x}}(Y)$ defined above is called* ***monodromy action****.*

This name became from the usual topological case, we can think this action as associating the "final point" of a "loop" (element of the étale fundamental group). A priori, this is only a way of think and is not actually how its defined.

Proposition 3.5.1. *Let $\varphi : Y \to X$ be a finite étale cover of X and $\overline{x} : Spec(k) \to X$ be a geometric point of X. The monodromy action of $\pi_1^{ét}(X, \overline{x})$ on $Fib_{\overline{x}}(Y)$ is continuous, where $Fib_{\overline{x}}(Y)$ is doted with the discrete topology (which coincides with the topology of the scheme $Y \times_X Spec(k)$).*

Proof. Since $Fib_{\overline{x}}(Y)$ has discrete topology, then show that the monodromy action is continuous is equivalent to show that for every $y \in Fib_{\overline{x}}(Y)$, the function

$$\begin{aligned} g_y : \pi^{ét}(X, \overline{x}) &\to Fib_{\overline{x}}(Y) \\ \sigma &\mapsto \sigma_Y(y), \end{aligned}$$

is a continuous function. Using that $Fib_{\overline{x}}(Y) \simeq \varinjlim_{P_\alpha \in \lambda} Hom(P_\alpha, Y)$ (see the section below to avoid confusion about notation and our conventions), then there exists $P_\alpha \in \Lambda$ and $\varphi \in Hom(P_\alpha, Y)$ such that y is identified with $[\varphi]$ (see the section below for details). Let

$$\begin{aligned} f_\alpha : \pi^{ét}(X, \overline{x}) &\to Aut(P_\alpha|X)^{op} \\ \sigma &\mapsto \sigma_{P_\alpha} \\ h_y : Aut(P_\alpha|X)^{op} &\to Fib_{\overline{x}}(Y) \\ \theta &\mapsto Fib_{\overline{x}}(\varphi \circ \theta)(p_\alpha); \end{aligned}$$

f_α and h_y are clearly continuous functions. Since $\varphi(\sigma_{P_\alpha})(p_\alpha) = y$ ($[\varphi]$ is the morphism identified with the point y!), then the next diagram is commutative

$$\begin{array}{ccc} \pi_1^{ét}(X, \overline{x}) & \xrightarrow{g_y} & Fib_{\overline{x}}(Y) \\ {\scriptstyle f_\alpha}\downarrow & \nearrow_{h_y} & \\ Aut(P_\alpha|X)^{op} & & \end{array}$$

Thus, g_Y is continuous. □

Definition 3.5.2. *Let G a profinite group. A G-**finite set** is a finite set X with a continuous action of G on X, where G have the profinite topology and X have the discrete topology. Morphism between G-finite sets are G-invariant maps. We denote by $G-finsets$ the category of G-finite sets.*

Let X be a scheme and $\overline{x}$ be a geometric point of X. The previous proposition show that for every finite étale cover Y of X, $Fib_{\overline{x}}(Y)$ is a $\pi_1^{\acute{e}t}(X,\overline{x})$-finite sets. Then, we can redefine the functor $Fib_{\overline{x}}$ by changing its target category

$$Fib_{\overline{x}} : F\acute{E}t_X \to \pi_1^{\acute{e}t}(X,\overline{x}) - finsets.$$

Theorem 3.5.1. ***(Grothendieck's geometrization of Galois theory)*** *Let X be a connected scheme and $\overline{x}$ be a geometric point of X. The functor*

$$Fib_{\overline{x}} : F\acute{E}t_X \to \pi_1^{\acute{e}t}(X,\overline{x}) - finsets,$$

is an equivalence of categories.

Proof. Only we need to prove that $Fib_{\overline{x}}$ is essentially surjective. Let E be a $\pi_1^{\acute{e}t}(X,\overline{x})$-finite set, we can suppose that the action of $\pi_1^{\acute{e}t}(X,\overline{x})$ on E is transitive (otherwise in this proof take the partition of E in orbits). Let $x \in E$ and let

$$Stab(x) = \{\sigma \in \pi^{\acute{e}t}(X,\overline{x}) | \sigma.x = x\},$$

be the stabilizer of x. If we denote by G the action of $\pi_1^{\acute{e}t}(X,\overline{x})$ on E, then we have that

$$Stab(x) = \pi_1^{\acute{e}t}(X,\overline{x}) \times \{x\} \cap G^{-1}(\{x\}),$$

then, using that E have discrete topology and G is a continuous function, then we have that $Stab(x)$ is an open subgroup of $\pi_1^{\acute{e}t}(X,\overline{x})$. Since $\pi_1^{\acute{e}t}(X,\overline{x})$ is a profinite group isomorphic to $\varprojlim_{\alpha\in\lambda} Aut(P_\alpha|X)^{op}$. Let , for every $\alpha \in \Lambda$, be the surjective function

$$\begin{aligned} f_\alpha : \pi_1^{\acute{e}t}(X,\overline{x}) &\to Aut(P\alpha|X)^{op} \\ \sigma &\mapsto \sigma_{P_\alpha} \end{aligned}$$

then $ker(f_\alpha)_{\alpha\in\Lambda}$ is a system of fundamental open neighborhoods of 1. Then there exists $\alpha \in \Lambda$, such that $ker(f_\alpha) \subseteq Stab(x)$. Let $U = f_\alpha(Stab(x))$, clearly U is an open subgroup of $Aut(P_\alpha|X)^{op}$, since $Aut(P_\alpha|X)^{op}$ is a discrete group. Let $Y = P_\alpha/U$ be the quotient of P_α by the group U, in previous sections we see that Y is a finite étale cover of X.

$Fib_{\overline{x}}(Y) \simeq E$: Since $Y = P_\alpha/U$, then the monodromy action of $\pi_1^{\acute{e}t}(X,\overline{x})$ on $Fib_{\overline{x}}(Y)$ can be factorized as the natural action of P_α on $Aut(P_\alpha|X)^{op}/U$, in particular, the monodromy action is transitive and therefore we have a bijection $Aut(Y|X) \simeq Fib_{\overline{x}}(Y)$. Thus

$$\begin{aligned} Fib_{\overline{x}}(Y) &\simeq Aut(Y|X) \\ &\simeq Aut(P_\alpha|X)^{op}/U \\ &\simeq \pi_1^{\acute{e}t}(X,\overline{x})/Stab(x) \\ &\simeq E \end{aligned}$$

the last bijection is a consequence of the Stabilizer-Orbit theorem and the hypothesis that the action on E is transitive. □

The next theorem is a deep Grothendieck's and beautiful generalization of Galois theory and justifies the name of the previous theorem.

Corollary 3.5.1. ***(Grothendieck-Galois theorem)*** *Let k be a field and k^{sep} be a separable closure inside of a algebraic closure $\overline{k}$. The functor,*

$$Hom_k(\_, k^{sep}) : F\acute{E}t_k \to Gal(k^{sep}|k) - finsets$$

is a coequivalence of categories.

Proof. $Hom_k(\_, k^{sep})$ and $Fib_{\overline{x}} \circ Spec(\_)$ are natural isomorphic, the last functor is the composition of an equivalence with a coequivalence and combine this with the fact that $\pi_1^{\acute{e}t}(Spec(k), \overline{x}) \simeq Gal(k^{sep}|k)$ and the assertion follows. □

At the beginning of this text was not clear what it mean exactly by a correct definition of a path or a loop in a scheme. Now, we know that the elements of the étale fundamental group are automorphisms of the fiber functor of a geometric point. Therefore, a loop in a scheme X with a base (geometric) point $\overline{x}$ can be understood by a natural isomorphism of $Fib_{\overline{x}}$. This is particular give us a notion of what a path in the algebro-geometric context will mean.

Definition 3.5.3. *Let X be a scheme and $\overline{x_1}, \overline{x_2}$ be geometric points of X. An* ***étale path*** *from $\overline{x_1}$ to $\overline{x_2}$ (or simply a* ***path****) is a natural isomorphism $F : Fib_{\overline{x_1}} \to Fib_{\overline{x_2}}$. In this section, as in the previous one, we conserve the notation and conventions about the étale fundamental group and the fiber functor.*

Proposition 3.5.2. *Let X be a connected scheme. If $\overline{x_1}$ and $\overline{x_2}$ are geometric points of X, then there exists an étale path from $\overline{x_1}$ to $\overline{x_2}$.*

Proof. $Fib_{\overline{x_1}}$ and $Fib_{\overline{x_2}}$ are pro-represented by the same objects only the morphisms between them can change. Explicitely, let $(P_\alpha, \phi_{\alpha,\beta})$ and $(P_\alpha, \psi_{\alpha,\beta})$ be inverse system of Galois coverings of X, representing $Fib_{\overline{x_1}}$ and $Fib_{\overline{x_2}}$, respectively. We want to construct a natural isomorphism from $Fib_{\overline{x_1}}$ to $Fib_{\overline{x_2}}$, thus it is sufficient to construct $\phi_\alpha \in Aut(P_\alpha|X)$, for every $\alpha \in \Lambda$, such that if $\alpha, \beta \in \Lambda$ with $\alpha \leq \beta$, then the next diagram is commutative

$$\begin{array}{ccc} P_\beta & \xrightarrow{\phi_\beta} & P_\beta \\ \downarrow{\scriptstyle \phi_{\alpha,\beta}} & & \downarrow{\scriptstyle \psi_{\alpha,\beta}} \\ P_\alpha & \xrightarrow[\phi_\alpha]{} & P_\alpha \end{array}$$

We can reduce it to prove that if $\alpha \leq \beta$ and we have $\phi_\beta \in Aut(P_\beta|X)$, then we can construct $\phi_\alpha \in Aut(P_\alpha|X)$, with the desired property. Let $q_\alpha = \psi_{\alpha,\beta}(\phi_\beta(p_\beta))$. Since P_α is a Galois

covering of X, then there exists a (unique) automorphism $\phi_\alpha \in Aut(P_\alpha, |X)$, such that $\phi_\alpha(p_\alpha) = q_\alpha$ (taking suitable geometric points of X).Therefore

$$\begin{aligned}\psi_{\alpha,\beta}(\phi_\beta(p_\beta)) &= q_\alpha \\ &= \phi_\alpha(p_\alpha) \\ &= \phi_\alpha(\phi_{\alpha,\beta}(p_\beta))\end{aligned}$$

thus $\psi_{\alpha,\beta} \circ \phi_\beta = \phi_\alpha \circ \phi_{\alpha,\beta}$. This completes the proof. □

Similarly to the case of topological spaces an étale path from $\overline{x_1}$ to $\overline{x_2}$ induces a continuous isomorphism $\pi_1^{ét}(X, \overline{x_1}) \to \pi_1^{ét}(X, \overline{x_2})$. Indeed
Let F be an étale path from $\overline{x_1}$ to $\overline{x_2}$. The function

$$\begin{aligned}\widetilde{F} : \pi_1^{ét}(X, \overline{x_1}) &\to \pi_1^{ét}(X, \overline{x_2}) \\ \sigma &\mapsto F \circ \sigma \circ F^{-1},\end{aligned}$$

is clearly an isomorphism of groups. Since $\widetilde{F}$ can be factorized through

$$\begin{aligned}\widetilde{F_\alpha} : Aut(P_\alpha|X)^{op} &\to Aut(P_\alpha|X)^{op} \\ \sigma_{Fib_{\overline{x}}(P_\alpha)} &\mapsto F_{Fib_{\overline{x}}(P_\alpha)} \circ \sigma_{Fib_{\overline{x}}(P_\alpha)} \circ F^{-1}_{Fib_{\overline{x}}(P_\alpha)},\end{aligned}$$

then $\widetilde{F}$ is continuous. In particular, we have the next corollary.

Corollary 3.5.2. ***(Independence of geometric points)*** *If X is a connected scheme, $\overline{x_1}$ and $\overline{x_2}$ are geometric points of X, then $\pi_1^{ét}(X, \overline{x_1})$ and $\pi_1^{ét}(X, \overline{x_2})$ are isomorphic as profinite groups.*

Therefore, if X is a connected scheme, then we can associate to X the following invariant (up to isomorphisms) $\pi_1^{ét}(X)$, where $\pi_1^{ét}(X) := \pi_1^{ét}(X, \overline{x})$, for some geometric point $\overline{x}$ of X. Notice that, the isomorphism defined below between étale fundamental groups of the same connected scheme with different geometric points is not natural (in the sense of category theory). For non-connected schemes we can associate an invariant too, the étale fundamental groupoid.

Definition 3.5.4. *Let X be an scheme. The* ***étale fundamental groupoid*** *is the category $\pi_1^{ét}(X)$ with objects $Fib_{\overline{x}}$, for every geometric point $\overline{x}$ of X and a morphism in $\pi_1^{ét}(X)$ is a natural isomorphism between this functors.*

4 The section conjecture

The process of thought, which feels and discovers, often blindly in the shadows, with sudden flashes of light when some tenacious false or simply inadequate image is finally shown for what it is, and things which seemed all crooked fall into place, with that mutual harmony which is their own.

Alexander Grothendieck

4.1 Anabelian geometry

In this section we revisited the first chapter of this text, adding geometric flavor to the main theorems of the first chapter and we use as a intuition to state the main conjectures in anabelian geometry. In the last chapter we see how étale fundamental groups are a vast generalization of Galois groups of fields and at the same time how are the correct analogue to fundamental groups in Algebraic geometry. We begin this geometric interpretation with the Artin-Schreier theorem

Theorem 4.1.1. ***(Artin-Schreier theorem)*** *Let k be a field. If $\pi_1^{\acute{e}t}(Spec(k), \overline{x})$ is a finite group for some geometric point $\overline{x}$ of $Spec(k)$, then we have only two options*

(i) $\pi_1^{\acute{e}t}(Spec(k), \overline{x})$ is trivial and k is algebraically closed, or

(ii) $\pi_1^{et}(Spec(k), \overline{x}) \simeq \mathbb{Z}/2\mathbb{Z}$ and k is real closed.

Thus Artin-Schreier theorem is now a theorem of rigidity of étale fundamental groups of fields: The finiteness condition on étale fundamental groups of a field is too rigid and impose field-theoretic conditions on how this field must be. This is an example of how group theoretic conditions on étale fundamental groups implies algebraic conditions (or equivalently geometric conditions) and this is part of the philosophy of the Anabelian geometry program. Another stronger result in this direction is the Neukirch-Uchida theorem that now can be restate as

Theorem 4.1.2. ***(Neuckirch-Uchida)*** *Let k and l be number fields, $\overline{x}$, $\overline{y}$ be geometric points of $Spec(k)$ and $Spec(l)$, respectively. k and l are isomorphic as fields if and only if $\pi_1^{\acute{e}t}(Spec(k), \overline{x})$ and $\pi_1^{\acute{e}t}(Spec(l), \overline{y})$ are isomorphic as profinite groups.*

In this case, we see that the isomorphy type of a number field is fully encoded in their étale fundamental group.
To finish this section we discuss and introduce basic ideas behind Anabelian geometry program. This program was introduced by Grothendieck in [8] and predicts the existence of some schemes for which their geometry and arithmetic are codified in their étale fundamental group. We present the conjectures of Grothendieck and some comments on its proofs.
The first anabelian conjecture proposed by Grothendieck and proved in full generality by Pop is the next theorem.

Theorem 4.1.3. ***(Grothendieck's birrational anabelian conjecture, Pop)*** *Let K and L be fields finitely generated over $\mathbb{Q}$. The function*

$$\begin{array}{rcl} Iso(K,L) & \to & Out(Gal_L, Gal_K) \\ \alpha & \mapsto & \alpha \circ \_ \circ \alpha^{-1}, \end{array}$$

is a bijection.

Note the similarity of this conjecture with the Galois characterization of number fields studied in the chapter 1 of this text. The Grothendieck's birrational anabelian conjecture remained open until Pop in [Pop] proves it. As well as the number field case the idea behind the proof is first establish a local correspondence. Of course, is not the same local correspondence that the number field case. Explicitly the idea is to take X and Y models of K and L, respectively and construct a birational invariants $\mathfrak{X}_K^1$, $\mathfrak{Y}_L^1$ of X and Y, respectively, in the following way

(i) First construct $\mathfrak{X}_K$, taking the projective limit of proper models of K. Similarly construct $\mathfrak{Y}_K$.

(ii) In this new spaces Pop give sense of what points of codimension k (for $k \in \mathbb{Z}$) means and take $\mathfrak{X}_K^1$ the points of $\mathfrak{X}_K$ of codimension 1.

(iii) The birational interpretation of $\mathfrak{X}_K^1$ is the set of valuations v of K, such that $Kr.dim(k(v)) = Kr.dim(K) - 1$ (here $Kr - dim(\_)$ is the Kronecker dimension, or equivalently the cohomological dimension minus one).

Now if $[\sigma] \in Out(Gal_L, Gal_K)$, then σ induces a correspondence

$$\varphi_\sigma : \mathfrak{X}_K^1 \to \mathfrak{Y}_L^1$$

The next in Pop's term is take back the geometry to this correspondence. To do that, a subset D of Zariski prime divisors of K is said **geometric** if there exists a quasi-projective, normal model X such that D is a subset of Wéil divisors of X, denote by $GeoDiv(K)$ be the set of geometric Zariski prime divisors of K. By Hironaka resolution of singualities theorem (recall that we are working in zero-characteristic) φ_σ induces a bijection $\varphi : GeoDiv(K) \to GeoDiv(L)$. And finally using induction on dimensions and Kummer theory we obtain the field isomorphism required from $K \to L$. Of course this is a not fair summary of Pop's prove, we strong recommend read the original prove in [43].
The previous Pop's theorem is also know as the zero-dimensional Grothendieck's anabelian conjecture before we state the next conjecture we need to introduce the next central definition.

Definition 4.1.1. *Let k be a perfect field. Let X be a smooth connected curve and $\widetilde{X}$ be a smooth completion of X. We say that X is a **hyperbolic curve** if $2g - 2 - r < 0$, where g is the genus of $\widetilde{X}$ and r is the cardinal of closed points of $\widetilde{X} \setminus X$.*

This curves are the objects that appears in the one dimensional Grothendieck's section conjecture. The next result makes sense to the name Anabelian

Proposition 4.1.1. *Let X be a curve over a field of characteristic zero. X is an hyperbolic curve if and only if $\pi_1^{\acute{e}t}(X_{\overline{k}}, \overline{x})$ is not abelian, for some geometric point $\overline{x}$ of $X_{\overline{k}}$.*

A vague idea behind Grothendieck's anabelian program is that for a scheme X if $\pi_1^{\acute{e}t}(X_{\overline{k}}, \overline{x})$ is less abelian, then more information about X is contained in this group and an anabelian scheme is a scheme that $\pi_1^{\acute{e}t}(X_{\overline{k},\overline{x})}$ the sufficiently not abelian to capture all the arithmetic and geometric information about X.

Theorem 4.1.4. ***(Grothendieck's curves anabelian conjecture, Tamagawa- Mochizuki)*** *Let X and Y be hyperbolic curves over field k, finitely generated over $\mathbb{Q}$. Then, the natural function (induced by functoriality of $\pi_1^{\acute{e}t}$)*

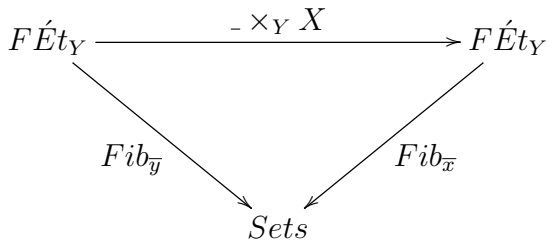
$$Iso(X, Y) \to Out(\pi_1^{\acute{e}t}(X, \overline{x}), \pi_1^{\acute{e}t}(Y, \overline{y})),$$

is a bijection.

This theorem has proved first in the affine case by Tamagawa in [55] and the general result proved by Mochizuki [**?**], and is much more difficult to understand than the case proved by Tamagawa, uses result in p-adic fields and then using methods of p-adic Hodge theory to complete the proof. But, as well as the previous cases one fundamental step is this two proofs is try to construct local correspondence, each one requires to develop a local theory and use different results to construct the desired isomorphism. If the reader wants to consult a great introduction to anabelian geometry, we recommend [44].

4.2 The exact homotopy sequence

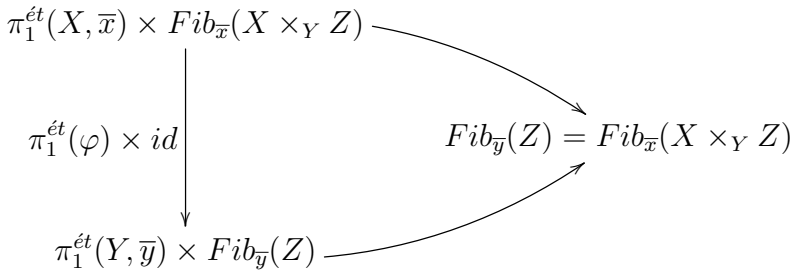
In this section we study a exact sequence which is fundamental to state and study Grothendieck's section conjecture. The exact homotopy sequence is a bridge between arithmetic and geometry, because this sequence involves Galois groups (coming from arithmetic) and fundamental groups coming from schemes over an algebraically closed fields. Before to state and prove the exactness of the homotopy sequence, we have to study some properties of $\pi_1^{\acute{e}t}$ as a functor. Recall that if $\varphi : X \to Y$ is morphism of schemes $\overline{x}$, $\overline{y}$ are geometric points of X, Y respectively and $\varphi(\overline{x}) = \overline{y}$, then the next diagram is commutative



Thus, the next homomorphism of groups is well-defined

$$\begin{aligned} \pi_1^{\acute{e}t}(\varphi) : \pi_1^{\acute{e}t}(X, \overline{x}) &\to \pi_1^{\acute{e}t}(Y, \overline{y}) \\ \sigma &\mapsto \pi_1^{\acute{e}t}(\sigma), \end{aligned}$$

where $\pi_1^{\acute{e}t}(\sigma)$ is the natural automorphism of $Fib_{\overline{y}}$, defined in a finite étale cover Z of Y as $\pi_1^{\acute{e}t}(\sigma)_{Fib_{\overline{y}}(Z)} = \sigma_{Fib_{\overline{x}}(X \times_Y Z)}$. Moreover, this homomorphism of groups commutes with the monodromy action, i.e., the next diagram is commutative



Definition 4.2.1. *Let X be an scheme. A finite étale covering Y of X is **trivial** if Y is isomorphic as X-scheme to $\bigsqcup_{i=1}^{n} X$, for some $n \in \mathbb{Z}^+$ (the structure morphism of $\bigsqcup_{i=1}^{n} X$ is $\bigsqcup_{i=1}^{n} id_X$).*

It is clear that the only X-automorphism of $\bigsqcup_{i=1}^{n} X$ is the identity and therefore the same is true for every trivial finite étale cover of X.
First, we study some geometric conditions on X are reflected as group properties of $\pi_1^{\acute{e}t}(X, \overline{x})$ or group properties of homomorphisms of fundamental groups.

Proposition 4.2.1. *Let X be a connected scheme and $\overline{x}$ be a geometric point of X. A finite étale covering Y of X is trivial if and only if the action of $\pi_1^{ét}(X,\overline{x})$ on $Fib_{\overline{x}}(Y)$ is trivial.*

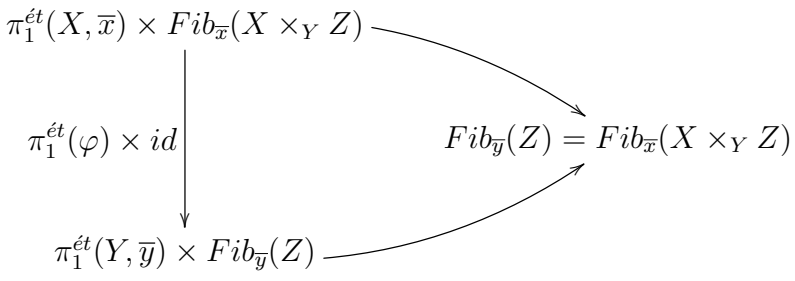
Proof. If Y is a trivial étale covering of X, the action of monodromy on $Fib : \overline{x}(Y)$ is defined by

$$\begin{aligned} \pi_1^{ét}(X,\overline{x}) \times Fib_{\overline{x}}(Y) &\to Fib_{\overline{x}}(Y) \\ (\sigma, y) &\mapsto \sigma_Y(y), \end{aligned}$$

but σ_Y is an X-automorphism of Y, as we see before it is the identity of Y. Therefore, the monodromy action in this case is trivial.
If the monodromy action of $\pi_1^{ét}(X,\overline{x})$ on $Fib_{\overline{x}}(Y)$ is trivial, let n be the cardinal number of the (finite) set $Fib_{\overline{x}}(Y)$, then $Fib_{\overline{x}}(\bigsqcup_{i=1}^{n} X)$ is a set of with n elements and therefore, there exists a bijection between $Fib_{\overline{x}}(Y)$ and $Fib_{\overline{x}}(\bigsqcup_{i=1}^{n} X)$, this bijection clearly preserves the action of $\pi_1^{ét}(X,\overline{x})$ because in each case it is trivial. Thus, $Fib_{\overline{x}}(Y)$ and $Fib_{\overline{x}}(\bigsqcup_{i=1}^{n} X)$ are isomorphic as $\pi_1^{ét}(X,\overline{x})$-finite sets, by Grothendieck's geometrization of Galois theory, we have that Y is isomorphic to $\bigsqcup_{i=1}^{n} X$ as X-schemes, i.e., Y is a trivial finite étale covering of X. □

Proposition 4.2.2. *Let $\varphi : X \to Y$ be a morphism of connected schemes, $\overline{x}$ and $\overline{y}$ be geometric points of X and Y, respectively such that $\varphi(\overline{x}) = \overline{y}$. $\pi_1^{ét}(\varphi)$ is the trivial group homomorphism if and only if for every finite étale cover Z of Y, then base change scheme $X \times_Y Z$ is a trivial finite étale cover of X.*

Proof. Suppose that $\pi_1^{ét}(\varphi)$ is the trivial group homomorphism. Since $\pi_1^{ét}(\varphi)$ fits in the next commutative diagram



then, the action of $\pi_1^{ét}(X,\overline{x})$ on $Fib_{\overline{x}}(X \times_Y Z)$ is trivial and therefore $X \times_Y Z$ is a trivial cover of X, by the previous proposition.
Reciprocally, suppose that for every finite étale covering Z of Y, the base change scheme $X \times_Y Z$ is a trivial cover of X, but $\pi_1^{ét}(\varphi)$ is not the trivial group homomorphism. Considering

the surjective group homomorphisms

$$\begin{aligned} f_\alpha : \pi_1^{\acute{e}t}(Y,\overline{y}) &\to Aut(P_\alpha|X)^{op} \\ \sigma &\mapsto \sigma_{P_\alpha}, \end{aligned}$$

we know that $\{ker(f_\alpha)\}_{\alpha\in\Lambda}$ is a fundamental system of open neighborhoods of 1, which intersection is $\{1\}$ (see chapter 2 for information about notation and our conventions). Therefore, there exists $\alpha \in \Lambda$, such that $\pi^{\acute{e}t}(\varphi)(\pi_1^{\acute{e}t}(X,\overline{x})) \not\subseteq ker(f_\alpha)$.
The first isomorphism theroem implies that $\pi_1^{\acute{e}t}(Y,\overline{y})/ker(f_\alpha)$ is a finite group, since it is isomorphic to the finite group $Aut(P_\alpha|X)^{op}$. Moreover, $\pi_1^{\acute{e}t}(Y,\overline{y})/ker(f_\alpha)$ is a $\pi_1^{\acute{e}t}(Y,\overline{y})$-finite set, where the action on this set is induced by the canonical quotient homomorphism. Using Grothendieck's geometrization of Galois theory, there exists a finite étale cover Z of Y, such that $Fib_{\overline{x}}(Y) \simeq \pi_1^{\acute{e}t}(Y,\overline{y})/ker(f_\alpha)$ as $\pi_1^{\acute{e}t}(Y,\overline{y})$-finite sets. The action of $\pi_1^{\acute{e}t}(X,\overline{x})$ on $Fib_{\overline{x}}(X\times_Y Z)$ is not trivial, since there exists $\sigma \in \pi_1^{\acute{e}t}(X,\overline{x})$ such that $\varphi(\sigma) \notin ker(f_\alpha)$ and using that

$$\begin{array}{ccc} \pi_1^{\acute{e}t}(X,\overline{x}) \times Fib_{\overline{x}}(X\times_Y Z) & & \\ \Big\downarrow \pi_1^{\acute{e}t}(\varphi)\times id & & Fib_{\overline{y}}(Z) = Fib_{\overline{x}}(X\times_Y Z) \\ \pi_1^{\acute{e}t}(Y,\overline{y}) \times Fib_{\overline{y}}(Z) & & \end{array}$$

is a commutative diagram, then $\sigma.\overline{1} \neq \sigma$ (if not $\varphi \in ker(f_\alpha)$). □

Proposition 4.2.3. *Let X be a connected scheme and $\overline{x}$ be a geometric point of X. A finite étale covering Y of X is connected if and only if the action of $\pi_1^{\acute{e}t}(X,\overline{x})$ on $Fib_{\overline{x}}(Y)$ is transitive.*

Proof. Suppose that Y is a connected finite étale covering of X. Let $\varphi : P_\alpha \to Y$ be the Galois closure of Y over X, then $Fib_{\overline{x}}(\varphi)$ is surjective. Since the next diagram is commutative

$$\begin{array}{ccc} \pi_1^{\acute{e}t}(X,\overline{x}) \times Fib_{\overline{x}}(P_\alpha) & \longrightarrow & Fib_{\overline{x}}(P_\alpha) \\ \Big\downarrow id\times Fib_{\overline{x}}(\varphi) & & \Big\downarrow Fib_{\overline{x}}(\varphi) \\ \pi_1^{\acute{e}t}(X,\overline{x}) \times Fib_{\overline{x}}(Y) & \longrightarrow & Fib_{\overline{x}}(Y) \end{array}$$

and the monodromy action on $Fib_{\overline{x}}(P_\alpha)$ is transitive (P_α is a Galois covering of X), then the action of $\pi_1^{\acute{e}t}(X,\overline{x})$ on $Fib_{\overline{x}}(Y)$ is transitive.
To prove the converse, suppose that $Fib_{\overline{s}}(Y)$ is a transitive $\pi_1^{\acute{e}t}(X,\overline{x})$-finite set.
Let $y \in Fib_{\overline{x}}(Y)$ and $\sigma \in \pi_1^{\acute{e}t}(X,\overline{x})$, then $\sigma_{Fib_{\overline{x}(Y)}}(y)$ is in the same connected component (of

Y) that y. Indeed, let C be the connected component of Y, of the point y, then C is a étale finite covering of X, the naturality of σ implies that the next diagram commutes

$$\begin{array}{ccc} Fib_{\overline{x}}(C) & \xrightarrow{\sigma_{Fib_{\overline{x}}(C)}} & Fib_{\overline{x}}(C) \\ \downarrow & & \downarrow \\ Fib_{\overline{x}}(Y) & \xrightarrow[\sigma_{Fib_{\overline{x}}(Y)}]{} & Fib_{\overline{x}}(Y) \end{array}$$

where the vertical arrows are the natural inclusions. Thus,

$$\sigma_{Fib_{\overline{x}(Y)}}(y) \;=\; \sigma_{Fib_{\overline{x}(C)}}(y) \in Fib_{\overline{x}}(C) \subseteq C,$$

Therefore if the action is transitive every two points must be in the same connected component, this completes the proof. □

Proposition 4.2.4. *Let $\varphi : X \to Y$ be a morphism of connected schemes, $\overline{x}$ and $\overline{y}$ be geometric points of X and Y, respectively such that $\varphi(\overline{x}) = \overline{y}$. $\pi_1^{\acute{e}t}(\varphi)$ is a surjective homomorphism group if and only if for every connected finite étale cover Z of Y, the change of base $Z \times_Y X$ is connected too.*

Proof. If $\pi_1^{\acute{e}t}$ is surjective. The commutative diagram

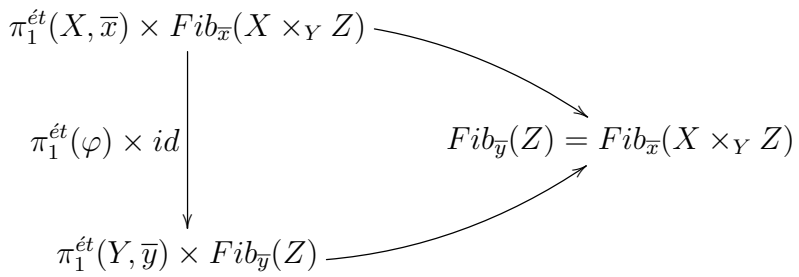
$$\begin{array}{ccc} \pi_1^{\acute{e}t}(X,\overline{x}) \times Fib_{\overline{x}}(X \times_Y Z) & & \\ \downarrow \pi_1^{\acute{e}t}(\varphi) \times id & \searrow & \\ & & Fib_{\overline{y}}(Z) = Fib_{\overline{x}}(X \times_Y Z) \\ \pi_1^{\acute{e}t}(Y,\overline{y}) \times Fib_{\overline{y}}(Z) & \nearrow & \end{array}$$

implies that, the action of $\pi_1^{\acute{e}t}(X,\overline{x})$ on $Fib_{\overline{x}}(X \times_Y Z)$ is transitive and therefore, $X \times_Y Z$ is connected.
Reciprocally suppose that for every finite étale cover Z of Y, the change of base $Z \times_X Y$ is a connected finite étale cover of X, but $\pi_1^{\acute{e}t}(\varphi)$ is not surjective. Recall that $\pi_1^{\acute{e}t}(X,\overline{x})$ and $\pi_1^{\acute{e}t}(Y,\overline{y})$ are profinite groups, then in particular are compact Hausdorff spaces. Then $Im(\pi_1^{\acute{e}t}(\varphi)$ is a closed subgroup of $\pi_1^{\acute{e}t}(Y,\overline{y})$. Considering the surjective group homomorphisms

$$\begin{array}{rcl} f_\alpha : \pi_1^{\acute{e}t}(Y,\overline{y}) & \to & Aut(P_\alpha|X)^{op} \\ \sigma & \mapsto & \sigma_{P_\alpha}, \end{array}$$

we know that $\{ker(f_\alpha)\}_{\alpha\in\Lambda}$ is a fundamental system of open neighborhoods of 1. Therefore, there exists $\alpha \in \Lambda$ such that $ker(f_\alpha) \cap (Im(\pi_1^{\acute{e}t}(\varphi)))^c = \emptyset$, equivalently, $ker(f_\alpha) \subseteq Im(\pi_1^{\acute{e}t}(\varphi))$.

Let $E = \pi_1^{ét}(Y,\overline{y})/Ker(f_\alpha)$ is a $\pi_1^{ét}(Y,\overline{y})$-finite set. Therefore, there exists a finite étale cover Z of Y, such that $Fib_{\overline{y}}(Z) \simeq E$, the commutativity of the next diagram



implies that, the action of $\pi_1^{ét}(X,\overline{x})$ on $Fib_{\overline{x}}(X \times_Y Z)$ is trivial. Therefore $X \times_Y Z$ is trivial but is not isomorphic to X, therefore it is disconnected. A contradiction, thus $\pi_1^{ét}(\varphi)$ is surjective. □

In a profinite group a subgroup is open if and only if it is closed of a finite index. In particular, if U is an open subgroup of $\pi_1^{ét}(X,\overline{x})$ (with X a connected scheme), then the quotient space $\pi_1^{ét}(X,\overline{x})/U$ is a $\pi_1^{ét}(X,\overline{x})$-finite set (the action on this set is induced by the canonical quotient map), moreover, the action on this set is transitive, we denote by Z_U a correspondent connected étale finite cover of X, i.e., such that $Fib_{\overline{x}}(Z_U) \simeq \pi_1^{ét}(X,\overline{x})/U$ (as $\pi_1^{ét}(X,\overline{x})$-finite sets).

Proposition 4.2.5. *Let $\varphi : X \to Y$ be a morphism between connected scheme and let U be an open subgroup of $\pi_1^{ét}(Y,\overline{y})$. $Im(\pi_1^{ét}(\varphi)) \subseteq U$ if, and only if the morphism $Z_U \times_Y X \to X$ has a section.*

Proof. Let $[z] \in \pi_1^{ét}(Y,\overline{y})/U$, since the action on this set is transitive, then

$$\pi_1^{ét}(Y,\overline{y})/U = Orb_{[z]},$$

by Stabilizer-orbit theorem,

$$\pi_1^{ét}(X,\overline{x})/Stab(z) \simeq (\pi_1^{ét}(Y,\overline{y})/U)/(Stab([z])/U) \simeq Orb_{[z]}$$

, without lose of generality we can suppose that $U = Stab(z)$. Then

$$\begin{aligned}
Im(\pi_1^{ét}(\varphi)) \subseteq U &\Leftrightarrow Im(\pi_1^{ét}(\varphi)) \subseteq Stab(z)\\
&\Leftrightarrow \pi_1^{ét}(X,\overline{x}) \text{ acts trivially on } z\\
&\Leftrightarrow \pi_1^{ét}(X,\overline{x}) \text{ acts trivially on a connected component } C \text{ of } X \times_Y Z\\
&\Leftrightarrow C \text{ is trivial and connected}\\
&\Leftrightarrow C \text{ is isomorphic to } X, \text{ as } X\text{-schemes}\\
&\Leftrightarrow \text{there exists an } X\text{-isomorphism} : X \to C\\
&\Leftrightarrow X \times_Y Z \to X \text{ has a section.}
\end{aligned}$$

Before continue we need to prove the next lemma about the topology of profinite groups. Recall that an closed subgroup of a profinite group is profinite too, se for example [17].

Lemma 4.2.1. *Let G be a profinite group and H be a closed subgroup of G.*

(i) $\cap\{H \subseteq K | K$ *is a open subgroup of* $G\} = H$.

(ii) If W is a open subgroup of H, then there exists an open subgroup V of G, such that $W = H \cap V$.

Proof. (i) Let $g \in G \setminus H$, $\{gN|N$ is an open normal subgroup of G is a fundamental system of open neighborhoods of g. Therefore, there exists an open normal subgroup N of G, such that gNH^c, or equivalently, $gN \cap H = \emptyset$. Recall that N is an open subgroup of G and therefore is a closed set of finite index. Consider the canonical quotient map

$$p : G \to G/N,$$

the quotient topology of G/N is discrete, since G/N is finite. In particular $p(H)$ is an open subgroup of G/N, then $p^{-1}(p(H))$ is a open subgroup of G containing H. If $g \in p^{-1}(p(H))$, then there exists $h \in H$, such that $p(g) = p(h)$, equivalently $h \in gH \cap H$, a contradiction. Therefore we find a open subgroup of G containing H but not g, this completes the proof.

(ii) W and H are, in particular, closed subgroups of G, therefore

$$\cap\{H \subseteq K | K \text{ is a open subgroup of } G\} = H, \text{ and}$$

$$\cap\{W \subseteq K | K \text{ is a open subgroup of } G\} = W.$$

Since $W \subseteq H$, then there exists a subset A of $\{W \subseteq K | K$ is a open subgroup of $G\}$ such that

$$W = \cap\{H \subseteq K | K \text{ is a open subgroup of } G\} \cap \bigcap_{V \in A} V;$$

but H is a profinite group too, therefore W has finite index in H, then A is finite, this completes the proof.

□

Proposition 4.2.6. *Let $\varphi : X \to Y$ be a morphism of connected schemes, $\overline{x}$ and $\overline{y}$ be geometric points of X and Y, respectively such that $\varphi(\overline{x}) = \overline{y}$ and let U be an open subgroup of $\pi_1^{\acute{e}t}(X, \overline{x})$. Then, $ker(\pi_1^{\acute{e}t}(\varphi)) \subseteq U$ if, and only if there exists a finite étale cover $Z \to Y$ and a X-morphism $Z_i \to Z_U$, where Z_i is a connected component of $Z \times_Y X$.*

Proof. We first prove the only if part of this lemma, because we use it in the if part. Suppose that there exists a finite étale cover $Z \to Y$ and a connected component Z_i of $Z \times_Y X$ with a X-morphism $\psi : Z_i \to Z_U$. The morphism ψ commutes with the monodromy actions, to be precise, the next diagram commutes

$$\begin{array}{ccc} \pi_1^{\acute{e}t}(X,\overline{x}) \times Fib_{\overline{x}}(Z_i) & \longrightarrow & Fib_{\overline{x}}(Z_i) \\ \downarrow{\scriptstyle id \times Fib_{\overline{x}}(\psi)} & & \downarrow{\scriptstyle id \times Fib_{\overline{x}}(\psi)} \\ \pi_1^{\acute{e}t}(X,\overline{x}) \times Fib_{\overline{x}}(Z_U) & \longrightarrow & Fib_{\overline{x}}(Z_U), \end{array}$$

On one hand the inclusion morphism $j : Z_i \hookrightarrow Z \times_Y X$ commutes with the monodromy action, as well as the homomorphism of groups $\pi_1^{\acute{e}t}(\varphi)$, i. e., the next diagrams are commutative

$$\begin{array}{ccc} \pi_1^{\acute{e}t}(X,\overline{x}) \times Fib_{\overline{x}}(Z_i) & \longrightarrow & Fib_{\overline{x}}(Z_i) \\ \downarrow{\scriptstyle id \times Fib_{\overline{x}}(j)} & & \downarrow \\ \pi_1^{\acute{e}t}(X,\overline{x}) \times Fib_{\overline{x}}(Z \times_Y X) & \longrightarrow & Fib_{\overline{y}}(Z) = Fib_{\overline{x}}(Z \times_Y X) \\ \downarrow{\scriptstyle \pi_1^{\acute{e}t}(\varphi) \times id} & \nearrow & \\ \pi_1^{\acute{e}t}(Y,\overline{y}) \times Fib_{\overline{y}}(Z) & & \end{array},$$

Let $z_u \in Fib_{\overline{x}}$ and $\sigma \in \pi_1^{\acute{e}t}(X,\overline{x})$, then there exists $z_i \in Fib_{\overline{x}}(Z_i)$, such that $\psi(z_i) = z_u$. Using the commutatitivity of the previous diagrams, we have that

$$\begin{aligned} \sigma.z_u &= \sigma.\psi(z_i) \\ &= \psi(\sigma.z_i) \\ &= \psi(\pi_1^{\acute{e}t}(\varphi)(\sigma).z_i) \\ &= \psi(1.z_i) \\ &= \psi(z_i) \\ &= z_u \end{aligned}$$

thus $\sigma.z_u = z_u$, equivalently $\sigma \in U$. Therefore, $ker(\pi_1^{\acute{e}t}(\varphi)) \subseteq U$.

Suppose that $ker(\pi_1^{\acute{e}t}(\varphi)) \subseteq U$. Let $W = \pi_1^{\acute{e}t}(\varphi)(U)$, as $\pi_1^{\acute{e}t}(Y,\overline{y})$ is compact and Hausdorff, then W is a closed subgroup of $\pi_1^{\acute{e}t}(Y,\overline{y})$. Since W has finite index in $Im(\pi_1^{\acute{e}t})$, then W is an open subgroup of $Im(\pi_1^{\acute{e}t})$, by the previous lemma there exists an open subgroup

V of $\pi_1^{ét}(Y,\overline{y})$, such that $W = V \cap Im(\varphi_1^{ét})$. Let Z_i be a connected component of $Z_V \times_Y X$, $Fib_{\overline{x}}(Z_i)$ is a transitive $\pi_1^{ét}(X,\overline{x})$-finite set. If $z \in Fib_{\overline{x}}(Z_i)$, then $Orb_z = Fib_{\overline{x}}(Z_i)$. By the orbit-stabilizer theorem $Fib_{\overline{x}}(Z_i) \simeq \pi_1^{ét}(X,\overline{x})/Stab(x)$, the stabilizer of x, $Stab(x)$, is an open subgroup of $\pi_1^{ét}(X,\overline{x})$. By the only if part, we know that $ker(\pi_1^{ét}(\varphi)) \subseteq Stab(x)$. We affirm that $Stab(x) \subseteq U$, since this two subgroups contains $ker(\pi_1^{ét}(\varphi))$, the previous affirmation is equivalent to prove that $\pi_1^{ét}(\varphi)(Stab(x)) \subseteq W$. Since the homomorphism

$$\begin{array}{rcl} \pi_1^{ét}(X,\overline{x})/Stab(x) & \to & \pi_1^{ét}(Y,\overline{y})/V \\ [t] & \mapsto & [\varphi_1^{ét}(t)], \end{array}$$

is well-defined (since Z_i is a connected component of $Z_V \times_Y X$). Then $\pi_1^{ét}(\varphi)(Stab(x)) \subseteq V$, intersecting on both sides with $Im(\pi_1^{ét}(\varphi))$, we have that $\pi_1^{ét}(\varphi)(Stab(x)) \subseteq W$, this concludes the proof. □

The proofs of the previous proposition shows that if Z is a connected finite étale cover of X, then $Fib_{\overline{x}}(Z) \simeq \pi_1^{ét}(X,\overline{x})/U$ for some open subgroup U of $\pi_1^{ét}(X,\overline{x})$ (indeed $U = Stab(z)$, for some element $z \in Fib_{\overline{x}}(Z)$). This remark and the previous proposition implies the next corollary.

Corollary 4.2.1. *With the same hypothesis of the previous proposition. $\pi_1^{ét}(\varphi)$ is injective if and only if for all connected finite étale cover $Z \to X$, there exists a finite étale cover $Z' \to Y$ and a X-morphism $Z_i \to Z$, where Z_i is a connected component of $Z' \times_Y Z$.*

Proof. This is a direct consequence of the previous proposition, since the interseccion of all the open subgroups of $\pi_1^{ét}(X,\overline{x})$ is trivial. □

Finally, we have a test to prove the exactness of sequences induced by the étale group functor.

Corollary 4.2.2. *Let $\varphi : X \to Y$ and $\psi : Y \to Z$ be morphisms between connected schemes, $\overline{x},\overline{y}$ and $\overline{z}$ be geometric points of X, Y and Z, respectively. The sequence of groups homomorphisms*

$$\pi_1^{ét}(X,\overline{x}) \xrightarrow{\pi_1^{ét}(\varphi)} \pi_1^{ét}(Y,\overline{y}) \xrightarrow{\pi_1^{ét}(\psi)} \pi_1^{ét}(Z,\overline{z}),$$

is exact if, and only if the next two conditions are satisfied

(i) For every finite étale cover Z' of Z, the finite étale cover $Z' \times_Z X$ is a trivial cover of X.

(ii) If Y' is a connected finite étale cover of Y, such that the base change morphism $Y' \times_Y X \to X$ has a section, then there exists a connected finite étale cover Z' of Z and a Y-morphism from a connected component of $Z' \times_Y X$ to Y'.

Finally we can state and proof the homotopy exact sequence. Only, we need one preliminar definition. In the rest of this section we fix a field k with an algebraic closure $\overline{k}$ and a separable closure k^{sep}.

Definition 4.2.2. *Let X be a k-scheme. We say that X is **geometrically integral**, if $X \times_{Spec(k)} Spec(k^{sep})$ is an integral scheme.*

Integral does not imply geometrically integral. For example, let $k = \mathbb{Q}$, $X = Spec(\mathbb{Q}[x]/x^2 + 2)$, then $X_{\mathbb{Q}^{sep}} = \{(x - \sqrt{2}), (x + \sqrt{2})\}$ is a discrete space, in particular, not irreducible and therefore not integral.
If X is a k-scheme, we denote by X_L the change of base scheme $X \times_{Spec(k)} Spec(L)$, where L is a field extension of k. In this text, an scheme is compact if every open covering has a finite refinement, we do not assume the Hausdorff hypothesis when we say that a scheme is compact.

Proposition 4.2.7. *Let X and Y be a compact and geometrically integral k-schemes. If $\varphi : Y_{k^{sep}} \to X_{k^{sep}}$ is a finite étale covering of $X_{k^{sep}}$, there exists a finite extension l of k, contained in k^{sep}, and a finite étale cover $Y^{'}$ of X_l, such that*

$$Y_{k^{sep}} \simeq Y^{'} \times_{Spec(l)} Spec(k^{sep}).$$

Proof. The compactness of X, implies that we can find a finite, open and affine cover of X, namely $\{Spec(A_i)\}_{i=1}^n$. Changing base of each element of this open affine covering we can construct a finite, open and affine cover of $X_{k^{sep}}$, to be precise $\{Spec(A_i \otimes_k k^{sep})\}_{i=1}^n$ is a finite open and affine cover of $X_{k^{sep}}$. As φ is finite étale (in particular affine), then $\varphi^{-1}(Spec(A_i \otimes_k k^{sep})) = Spec(B_i)$, where B_i is a finitely presented $A_i \otimes_k k^{sep}$- module, then there exists $m, r \in \mathbb{Z}^+$, such that

$$B_i \simeq A_i \otimes_k [x_1, ..., x_m]/ \langle f_1, ..., f_r \rangle,$$

for some polynomials $f_1, ..., f_r \in B_i \simeq A_i \otimes_k [x_1, ..., x_m]$. For every $j \in \{1, ..., r\}$, let $C_{i,j}$ be the finite subset of $A_i \otimes_k k^{sep}$ which elements are the coefficients of the polynomial f_j. Let C be the finitely generated k^{sep} algebra generated by $\bigcup_{j=1}^{r} C_{i,j}$. Then

$$C_i \simeq k^{sep}[y_1, ..., y_k]/ \langle g_1, ..., g_t \rangle,$$

let L_i be the finite extension of k generated by the coefficients of $g_1, ..., g_t$ (it is finite since the coefficients of this polynomials belongs to k^{sep}). Then

$$B_i \simeq (A_i \otimes_k L_i[x_1, ..., x_m]/ \langle f_1, ..., f_r \rangle) \otimes_{L_i} k^{sep},$$

varying the index i we can construct a finite extension L of k, sufficiently large such that the previous isomorphism holds for every i. The proof finish when we prove that this isomorphisms are coherent, then using cocycles conditions we can contruct $Y^{'}$ gluing this spectra. □

Let X be k-variety and $\overline{x} : Spec(\overline{k}) \to X$ be a geometric point of X. $\overline{x}$ induces a geometric point (that we denote in the same way) $\overline{x} : Spec(\overline{k}) \to X_{k^{sep}}$ in $X_{k^{sep}}$ and the inclusion $k \hookrightarrow \overline{k}$, induces a geometric point on $Spec(k)$ (that we denote in the same way). Fixing this (three) geometric point $\overline{x}$, the natural morphism $X_{k^{sep}} \to X$ and the structure morphism $X \to Spec(k)$ combined with the functoriality of $\pi_1^{\acute{e}t}$, induces a sequence of groups homomorphism

$$\pi_1^{\acute{e}t}(X_{k^{sep}}, \overline{x}) \to \pi_1^{\acute{e}t}(X, \overline{x}) \to \pi_1^{\acute{e}t}(Spec(k), \overline{x}),$$

but, we know that $\pi_1^{\acute{e}t}(Spec(k), \overline{x})$ is isomorphic to the absolute Galois group Gal_k of k, identifying this groups, the previous sequence can be rewritten by

$$\pi_1^{\acute{e}t}(X_{k^{sep}}, \overline{x}) \to \pi_1^{\acute{e}t}(X, \overline{x}) \to Gal_k,$$

we call this sequence **the homotopy sequence**.

Theorem 4.2.1. ***(Homotopy exact sequence)*** *Let X be a compact geometrically integral k-scheme. The homotopy sequence*

$$1 \to \pi_1^{\acute{e}t}(X_{k^{sep}}, \overline{x}) \to \pi_1^{\acute{e}t}(X, \overline{x}) \to Gal_k \to 1$$

is exact.

Proof. Denote by $p : X_{k^{sep}} \to X$ the canonical projection morphism and $\varphi : X \to k$ the structure morphism of X as k-scheme. We divide this proof in three steps

Step 1: $\pi_1^{\acute{e}t}(p)$ is injective. Let $Y \to X_{k^{sep}}$ be a connected finite étale cover of $X_{\overline{k}}$, by the previous proposition, there exists a finite extension L of k contained in k^{sep} and a finite étale cover $Y^{'}$ of X_L, such that $Y \simeq Y^{'} \times_{Spec(L)} Spec(k^{sep})$. Note that X_L is a finite étale cover of X, since X_L is the base change (by X) of the finite étale morphism $Spec(L) \to Spec(k)$ (L is a finite separable extension of k) induced by the inclusion map $k \hookrightarrow L$. Then, $Y^{'}$ is a finite étale cover of X. Let C be a connected component of $Y^{'} \times_{Spec(L)} Spec(k^{sep})$, then there exists a morphism $C \to Y$ (is the composition of the inclusion morphism $C \hookrightarrow Y^{'} \times_{Spec(L)} Spec(k^{sep})$ and an isomorphism $Y^{'} \times_{Spec(L)} Spec(k^{sep}) \to Y$). Thus Proposition 4.2.1 implies that $\pi_1^{\acute{e}t}(p)$ is a injective group homomorphism.

Step 2: $\pi_1^{\acute{e}t}(\varphi)$ is surjective. Let $Z \to Spec(k)$ be a connected finite étale cover of $Spec(k)$, we need to prove that the base change $X \times_{Spec(k)} Z$ is connected too. Since Z is a connected finite étale cover of the spectrum of a field, then Z is isomorphic as $Spec(k)$-scheme to $Spec(L)$, where L is a finite separable extension of k, without lose of generality we can suppose that L is contained in k^{sep}. Then $X \times_{Spec(k)} Z \simeq X_L$, as X is geometrically integral, then $X_{k^{sep}}$ is integral, in particular, it is connected, there exists a surjective morphism $X_{k^{sep}} \to X_L$, then X_L is connected. Proposition 4.2.4 concludes step 2.

Step 3 Exactness in the middle. Only remains to prove that

$$\pi_1^{ét}(X_{k^{sep}}, \overline{x}) \to \pi_1^{ét}(X, \overline{x}) \to Gal_k,$$

is exact. Via Proposition 4.2.2 we show this by proving the next two conditions.

(i) Let $Z \to k$ be a finite étale cover of $Spec(k)$. We need to prove that $Z \times_S pec(k) X_{k^{sep}}$ is a trivial cover of $X_{k^{sep}}$. Indeed, since Z is a finite étale cover of the spectrum of a field, then Z is the spectrum of a finite étale k-algebra, therefore there exists $k_1, ..., k_n$ finite separable field extensions of k such that $Z \simeq \bigsqcup_{i=1}^{n} Spec(k_i)$. We can suppose that $k_i k^{sep}$ for every $i \in \{1, ..., n\}$. Then

$$\begin{aligned}
X_{k^{sep}} \times_{Spec(k)} &\simeq X_{k^{sep}} \times_{Spec(k)} \bigsqcup_{i=1}^{n} Spec(k_i) \\
&\simeq \bigsqcup_{i=1}^{n} X_{k^{sep}} \times_{Spec(k)} Spec(k_i) \\
&\simeq \bigsqcup_{i=1}^{n} X \times_{Spec(k)} Spec(k^{sep}) \times_{Spec(k)} Spec(k_i) \\
&\simeq \bigsqcup_{i=1}^{n} X \times_{Spec(k)} Spec(k^{sep} \otimes_k k_i) \\
&\simeq \bigsqcup_{i=1}^{n} X \times Spec(k^{sep}) \\
&\simeq \bigsqcup_{i=1}^{n} X_{k^{sep}},
\end{aligned}$$

This prove this first condition.

(ii) We can reduce the second condition of Proposition 4.2.2 to Galois coverings,i. e., is we prove the second (ii) of Proposition 4.2.2 then the same is true to connected finite étale cover, since every connected finite étale cover has a Galois covering.
Let $\varphi : Z \to X$ be a Galois covering of X, such that $Z \times_X X_{k^{sep}} \to X_{k^{sep}}$ has a section. Since X is geometrically integral, then X is integral, let η be the generic point of X, the generic fiber $Z \times_X Spec(k(\eta))$ ($k(\eta)$ is the residual field of X at the point η or equivalently, the function field of X) is a finite étale cover of $Spec(k(\eta))$, then it is the spectrum of a finite Galois extension K of $k(\eta)$. Thus $K \otimes_k k^{sep} \simeq \prod_{i \in I} k^{sep}(\eta)$, for some finite set I, therefore $K \simeq k(\eta) \otimes_k L$, for some finite Galois extension L of k. The finite étale cover X_L of X, is actually a Galois cover of X (since L is Galois extension of k). The function field of X_L is $K \otimes L$, the same as Y, therefore we have an isomorphism between Y and X_L over generic points, equivalently, there exists an open and dense subset U of X, such that $X_L \times_X U \simeq Y \times_X U$, but X_L and Y are locally free over U (since are finite étale covers), thus $X_L \simeq Y$. This completes this proof.

□

Corollary 4.2.3. *Let X be a compact and geometrically integral k-scheme. There exists a continuous homomorphism of groups.*

$$\rho_X : Gal_k \rightarrow Out(\pi_1^{ét}(X_{k^{sep}}, \overline{x})).$$

Proof. We identify $\pi_1^{ét}(X_{k^{sep}}, \overline{x})$ with a normal subgroup of $\pi_1^{ét}(X, \overline{x})$ using the previous theorem. Let

$$\begin{aligned} \varphi : \pi_1^{ét}(X, \overline{x}) &\rightarrow Aut(\pi_1^{ét}(X_{k^{sep}}, \overline{x})) \\ \sigma &\mapsto \varphi_\sigma, \end{aligned}$$

where $\varphi_\sigma(\theta) = \sigma \circ \theta \circ \sigma^{-1}$. Note that $\varphi(\pi_1^{ét}(X_{k^{sep}}, \overline{x})) = Inn(\pi_1^{ét}(X_{k^{sep}}, \overline{x}))$. Then φ induces a well defined homomorphism of groups

$$\widetilde{\varphi} : \pi_1^{ét}(X, \overline{x})/\pi_1^{ét}(X_{k^{sep}}, \overline{x}) \rightarrow Aut(\pi_1^{ét}(X_{k^{sep}}, \overline{x}))/Inn(\pi_1^{ét}(X_{k^{sep}}, \overline{x})),$$

using the exactness of the homotopy sequence we know that

$$\pi_1^{ét}(X, \overline{x})/\pi_1^{ét}(X_{k^{sep}}, \overline{x}) \simeq Gal_k.$$

Then, after compose with this isomorphism we obtain a homomorphism of groups

$$\rho_X : Gal_k \rightarrow Out(\pi_1^{ét}(X_{k^{sep}}, \overline{x})).$$

□

Definition 4.2.3. *Let X be a compact geometrically connected scheme. The homomorphism of the previous lemma*

$$\rho_X : Gal_k \rightarrow Out(\pi_1^{ét}(X_{k^{sep}}, \overline{x})).$$

is called the ***outer Galois action*** *of $\pi_1^{ét}(X_{k^{sep}}, \overline{x})$.*

As we see in the section 1 the absolute Galois group of the rational numbers $Gal(\overline{\mathbb{Q}}|\mathbb{Q})$ codifies the arithmetic of number fields, precisely we see how the isomorphy type of a number field is codified as the isomorphism of some subgroup of $Gal(\overline{\mathbb{Q}}|\mathbb{Q})$. This object is central in Grothendieck's Esquisse d'un programme [8], one part of this program is anabelian geometry, but there is other parts of this program that are related between them, for example, Grothendieck-Teichmuller theory or Dessins D'enfants, then, Grothendieck's Anabelian geometry is a part of a much larger plan of understand geometrically $Gal(\overline{\mathbb{Q}}|\mathbb{Q})$. To finish this section we state Belyi's theorem whose proof is in [49], we are not focus in the proof, but in a consequence which connects arithmetic and topology using the outer Galois action and begin Grothendieck's Dessins d'enfants whose idea is use combinatorial ideas to describe actions of $Gal(\overline{\mathbb{Q}}|\mathbb{Q})$ on some Riemann surfaces. For a comprehensible introduction we recomend [5].

Definition 4.2.4. *Let X be k-scheme and l be a subfield of k. We say that X* ***can be defined over*** *l if there exists an l-scheme X_0, such that $X_0 \times_{Spec(l)} Spec(k) \simeq X$.*

Theorem 4.2.2. ***(Belyi's theorem)*** *Let X be an integral proper normal curve defined over an algebraically closed of characteristic 0. X can be defined over $\mathbb{Q}$ if and only if there exists a morphism $X \to \mathbb{P}^1_k$, étale over $\mathbb{P}^1_k \setminus \{0,1,\infty\}$.*

Corollary 4.2.4. *The outer Galois action*

$$\rho_{\mathbb{P}^1_{\mathbb{Q}}\setminus\{0,1,\infty\}} : Gal_{\mathbb{Q}} \to Out(\pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1\infty\}, \overline{x}))$$

is injective.

Proof. We denote, in this proof, $\rho_{\mathbb{P}^1_{\mathbb{Q}}\setminus\{0,1,\infty\}}$ by ρ. Since ρ is continuous, then $ker(\rho)$ is a closed subgroup of $Gal(\overline{\mathbb{Q}}|\mathbb{Q})$. Using Galois infinite theory, there exists a subfield L of $\overline{\mathbb{Q}}$, such that $Gal(\overline{\mathbb{Q}}|L) = ker(\rho)$. Thus, $\rho|_{Gal(\overline{\mathbb{Q}}|L)}$ is the trivial homomorphism. Since L is a subfield of $\overline{\mathbb{Q}}$, then $Gal(\overline{\mathbb{Q}}|L)$ is the absolute Galois group of L. Moreover, $\rho|_{Gal(\overline{\mathbb{Q}|L})} = \rho_{\mathbb{P}^1_L\setminus\{0,1,\infty\}}$, denote this homomorphism by ρ_L. Recall that ρ_L comes from the homotopy exact sequence

$$1 \to \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1\infty\}, \overline{x}) \to \pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x}) \to Gal_L \to 1$$

Explicitely,

$$\begin{array}{rccl} \rho_L : Gal_L \simeq \pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x})/\pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1\infty\}, \overline{x}) & \to & Out(\pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1\infty\}, \overline{x})) \\ \sigma & \mapsto & [\rho_\sigma], \end{array}$$

where $\rho_\sigma(\theta) = \sigma \circ \theta \circ \sigma^{-1}$, for every $\sigma \in \pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x})$. Since ρ_L is trivial, then for every $\sigma \in \pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x})$, ρ_σ is a inner automorphism of $\pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x})$. Let

$$C = \{\theta \in \mathbb{P}^1_L \setminus \{0,1\infty\}, \overline{x}) | \theta \circ \varphi = \varphi \circ \theta, \text{ for all } \varphi \in \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1\infty\}, \overline{x})\}.$$

Since ρ_σ is a inner automorphism of $\pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x})$, then there exists $\sigma_1 \in \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x})$, such that $\rho_\sigma = Inn(\sigma_1)$ (the inner automorphism defined by conjugation by σ_1), or equivalently, $\sigma_1^{-1} \circ \sigma \in C$. This implies that

$$\pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x}) = \Big\langle C \cup \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x}) \Big\rangle.$$

On the other hand $C \cap \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x})$ is clearly a subgroup of the center of $\pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x})$. Now, we use the follow theorem whose proof can be found in [16].

Theorem 4.2.3. *Let $k \to l$ be a homomorphism between algebraically closed fields of characteritic zero. If X is a normal, quasi-projective k-scheme, then the homomorphism, induced by change of base, $\pi_1^{\acute{e}t}(X_l, \overline{x}) \to \pi_1^{\acute{e}t}(X, \overline{x})$ is an isomorphism of groups.*

Then, $\pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x}) \simeq \pi_1^{\acute{e}t}(\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}, \overline{x})$. But in a past section we see that $\pi_1^{\acute{e}t}(\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}, \overline{x})$ is the profinite completion of a free group on two generators, in particular, $\pi_1^{\acute{e}t}(\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}, \overline{x})$ have trivial center. Thus, $C \cap \pi_1^{\acute{e}t}(\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}, \overline{x}) = \{0\}$. Therefore,

$$\pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x}) \simeq C \times \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x}).$$

Let

$$p : \pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x}) \to \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x}).$$

be the projection on the second factor. We can construct a functor

$$p_* : \pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x}) - finsets \to \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x}) - finsets,$$

in the following way: For every $\pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x})$ -finite set E, $p_*(E)$ as a set is just E and the action on $p_*(E)$ is a retract the action of $\pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x})$ over E by p. Explicitely.

$$\begin{aligned} \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x}) \times E &\to E \\ (\theta, x) &\mapsto p(\theta).x, \end{aligned}$$

(on the right side of the previous function $p(\rho).x$ means the action on E as $\pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x})$-finite set). Since p is a left inverse of the natural homomorphism

$$\pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x}) \hookrightarrow \pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x})$$

then p_* is essentially surjective.
Clearly, p_* fits in the next commutative diagram

$$\begin{array}{ccc} F\acute{E}t_{\mathbb{P}^1_L \setminus \{0,1,\infty\}} & \xrightarrow{- \otimes_{Spec(L)} Spec(\overline{\mathbb{Q}})} & F\acute{E}t_{\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}} \\ \downarrow Fib_{\overline{x}} & & \downarrow Fib_{\overline{x}} \\ \pi_1^{\acute{e}t}(\mathbb{P}^1_L \setminus \{0,1,\infty\}, \overline{x}) - finsets & \xrightarrow[p_*]{} & \pi_1^{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overline{x}) - finsets \end{array}$$

since the vertical arrows are equivalence of categories. Then the base change functor is surjective. By Belyi's theorem this implies that every proper normal curve defined over $\overline{\mathbb{Q}}$ can be defined over L. If $L \subsetneq \overline{\mathbb{Q}}$, this is false. Indeed let $j \in \overline{\mathbb{Q}} \setminus L$, by [52], we can construct an elliptic curve E with j as his j-invariant. If E can be defined over L, then there exists a curve X such that $X_{\overline{\mathbb{Q}}} \simeq E$, since E is an elliptic curve, then X must be a curve of genus 1, therefore if F is the Jacobian of X, then F is an elliptic curve defined over L, but the j-invariant does not change, i.e., $j(F) = j(E) = j$. This is a contradiction, since F is defined over L implies that its j-invariant is an element of L. Thus $L = \overline{\mathbb{Q}}$ and $ker(\rho) = Gal(\overline{\mathbb{Q}}|\overline{\mathbb{Q}})$, this concludes the proof. □

4.3 Grothendieck's section conjecture

In this section, k denote a field, $\overline{k}$ an algebraic closure of k, and k^{sep} the separable extension of k inside of $\overline{k}$.

Definition 4.3.1. *Let X be a $k-$scheme and L be a field. A L-**rational** point of X is a k-morphism $X : Spec(L) \to X$. The set of L-rational points of X is denoted by $X(L)$.*

Let X be a compact, geometrically connected k-scheme. If $x : Spec(k) \to X$ is a k-rational point of X, then x is a section of the structure morphism $\rho : X \to Spec(k)$ of X. The inclusion map $k \hookrightarrow \overline{k}$, induces a morphism $f : Spec(\overline{k}) \to Spec(k)$ and therefore $\overline{x} := x \circ f$ is a geometric point of X. Therefore, x induces a group homomorphism

$$\pi_1^{\acute{e}t}(x) : Gal_k \to \pi_1^{\acute{e}t}(X, \overline{x})$$

which is a section of the exact homotopy sequence

$$1 \to \pi_1^{\acute{e}t}(X_{k^{sep}}, \overline{x}) \to \pi_1^{\acute{e}t}(X, \overline{x}) \to Gal_k \to 1,$$

(indeed, $\pi_1^{\acute{e}t}(x)$ is a section of this sequence, since x is a section of ρ and $\pi_1^{\acute{e}t}$ is a functor). We denote by s_x the morphism $\pi_1^{\acute{e}t}(x)$.

For a geometric point $\overline{y}$ we denote by $Sec_{\pi_1^{\acute{e}t}(X|k,\overline{y})}$ be set of group theoretic sections of the homotopy exact sequence

$$1 \to \pi_1^{\acute{e}t}(X_{k^{sep}}, \overline{y}) \to \pi_1^{\acute{e}t}(X, \overline{y}) \to Gal_k \to 1.$$

We want to construct from $X(k)$ to the set $Sec_{\pi_1^{\acute{e}t}(X|k,\overline{y})}$, one first idea is define the next "function "

$$\begin{array}{rcl} X(k) & \to & Sec_{\pi_1^{\acute{e}t}(X|k,\overline{y})} \\ x & \mapsto & s_x, \end{array}$$

but this is not well defined function, since in the previous construction we see that the geometric point $\overline{x}$ where the section $s_x : Gal_k \to \pi_1^{\acute{e}t}(X, \overline{x})$ is defined depends on x. So we need to avoid the dependence of the previous morphism on the geometric point $\overline{x}$.

Let $\overline{y}$ be a fixed geometric point of X, if $x \in X(k)$, we denote by $\overline{x}$ be the geometric point of X constructed above. There exists an étale path $\varphi : Fib_{\overline{x}} \to Fib_{\overline{y}}$, which induces a continuous group isomorphism

$$\begin{array}{rcl} \widetilde{\varphi} : \pi_1^{\acute{e}t}(X, \overline{x}) & \to & \pi_1^{\acute{e}t}(X, \overline{y}) \\ \sigma & \mapsto & \varphi \circ \sigma \circ \varphi^{-1}, \end{array}$$

Notice that $\pi_1^{\acute{e}t}(\rho) \circ \widetilde{\varphi} = \pi_1^{\acute{e}t}(\rho)$, where ρ is the structure morphism of X as a k-scheme. This isomorphism allow us to construct a group section of $\pi_1^{\acute{e}t}(X, \overline{y}) \to Gal_k$ from x, defined by $\widetilde{\varphi} \circ s_x$ and noted by $s_{x,\varphi}$. Now, this section depends on the choice of the étale path φ, we need to know when two étale path produces the same section. For this purpouses we defined the next equivalence relation on $Sec_{\pi_1^{\acute{e}t}(X|k,\overline{y})}$; for sections s, t of the homotopy exact sequence (with basepoint $\overline{y}$), we say that s and t are equivalent if and only if there exists $\sigma \in \pi^{\acute{e}t}(X_{k^{sep}}, \overline{x})$, such that $\sigma \circ s \circ \sigma^{-1} = t$ and we denote by $\mathcal{S}_{\pi_1^{\acute{e}t}(X|k,\overline{y})}$ the set of equivalence classes.

Proposition 4.3.1. *Let X be a compact geometrically connected k-scheme. If $\overline{x}, \overline{y}$ are geometric points of X, then $Sec_{\pi_1^{ét}(X|k,\overline{x})} \simeq Sec_{\pi_1^{ét}(X|k,\overline{y})}$.*

Proof. Let φ be an étale path from $\overline{x}$ to $\overline{y}$, then

$$\begin{array}{rcl} \overline{\varphi} : \mathcal{S}_{\pi_1^{ét}(X|k,\overline{x})} & \to & \mathcal{S}_{\pi_1^{ét}(X|k,\overline{y})} \\ [s] & \mapsto & [\widetilde{\varphi}(s)], \end{array}$$

is a well-defined bijection (with inverse $\overline{\varphi^{-1}}$). □

Proposition 4.3.2. *Let X be a compact geometrically connected k-scheme and let $\overline{y}$ be a geometric point. If $x \in X(k)$ and $\overline{x}$ is the associated geometric point of x, then for every two étale paths φ, ψ from $\overline{x}$ to $\overline{y}$ we have that $[\widetilde{\varphi}(s_x)] = [\widetilde{\psi}(s_x)]$.*

Proof. Let $\sigma = \psi \circ \varphi^{-1}$, it is clear that $\sigma \circ \widetilde{\varphi}(s_x) \circ \sigma^{-1} = \widetilde{\psi}(s_x)$. □

Definition 4.3.2. *Let X be a compact geometrically connected k-scheme and let $\overline{y}$ be a geometric point. The **profinite Kummer map** κ_X of X, is the function defined by*

$$\begin{array}{rcl} \kappa_X : X(k) & \to & \mathcal{S}_{\pi_1^{ét}(X|k,\overline{y})} \\ x & \mapsto & [\widetilde{\varphi}(s_x)], \end{array}$$

where φ is an étale path from $\overline{x}$ (the geometric point associated to x) to $\overline{y}$.

Finally we have all the tools to enunciate Grothendieck's section conjecture.

Conjecture 4.3.1. ***(Grothendieck's section conjecture)*** *Let X be a smooth, projective k- curve or genus at least 2 , where k finitely generated over $\mathbb{Q}$. The profinite Kummer map κ_X of X is a bijection.*

Then, the idea behind the section conjecture is that if we growth our knowledge about group theoretic sections of exact sequence, then the section conjecture would imply a better understanding of k-rational points (at least in this special type of curves) that bring back a new point of view to difficult and old problems in arithmetic, specially in arithmetic geometry. But Grothendieck's section conjecture is a big mistery, not much is known about this conjecture. To finalize this section we summarize some known results around this difficult and mysterious conjecture.

Definition 4.3.3. *Let Γ be a profinite group. A Γ-group is a profinite group N qith a group homomorphism $\rho : \Gamma \to Aut(N)$, such that the induced action*

$$\begin{array}{rcl} \Gamma \times N & \to & N \\ (g, n) & \mapsto & \rho_g(n), \end{array}$$

*is continuous, where $\rho_g = \rho(g)$. We refer to ρ as the **structure homomorphism** of N.*

If N is a Γ-group with structure homomorphism ρ, we can construct a new group called the **semidirect product** of N and Γ, denoted by $N \rtimes_\rho \Gamma$. As a set $N \rtimes_\rho \Gamma$ is just the cartesian product $N \times \Gamma$, but the operation on this set is modified by the rule

$$(n_1, g_1)(n_2, g_2) = (n_1 \rho_{g_2}(n_2), g_1 g_2),$$

This groups fits in the exact sequence

$$1 \to N \to N \rtimes_\rho \Gamma \to \Gamma \to 1,$$

defined in the canonical way. The previous exact sequence is equipped with a canonical (continuous) section

$$\begin{aligned} c : \Gamma &\to N \rtimes_\rho \Gamma \\ g &\to (1, g), \end{aligned}$$

and thus is a split exact sequence. Reciprocally every split exact sequence occurs in this way. To be explicit, we have the next proposition.

Proposition 4.3.3. *Let*

$$1 \to N \to \Pi \to \Gamma \to 1,$$

be a exact sequence of profinite groups. If $s : \Gamma \to \Pi$ is a section of $\Pi \to \Gamma$, then N is a Γ-group for some structure homomorphism ρ^s, such that $\Pi \simeq N \rtimes_{\rho^s} \Gamma$.

Proof. Let $s : \Gamma \to \Pi$ be a section of $j : \Pi \to \Gamma$ (the homomorphism appearing in the exact sequence). Using the previous exact sequence we identify N as a subgroup of Π, this subgroup is characterized to be $ker(j)$.
Let

$$\begin{aligned} \rho^s : \Gamma &\to Aut(N) \\ g &\mapsto \rho^s_g, \end{aligned}$$

where $\rho^s_g(n) = s(g) n s(g)^{-1}$, for every $n \in N$. Note that

$$\begin{aligned} j(\rho^s_g(n)) &= j(s(g) n s(g)^{-1}) \\ &= j(s(g)) j(n) j(s(g)^{-1}) \\ &= g 1 g^{-1} \\ &= 1, \end{aligned}$$

then $j(\rho_g(n)) = 1$, or equivalently, $\rho^s_g(n) \in N$. Thus ρ^s is well-defined. Now, define

$$\begin{aligned} F_s : N \rtimes_{\rho^s} \Gamma &\to \Pi \\ (g, n) &\to s(g) n, \end{aligned}$$

Is not difficult to prove that F_s is a group isomorphism. □

For the rest of this section we keep the notation of the previous proof. Note that if s is a section of a exact sequence

$$1 \to N \to \Pi \to \Gamma \to 1,$$

then under the (inverse of the) isomorphism $F_s : N \times_{\rho_s} \Gamma \to \Pi$, s is identified with the canonical section $c_s : \Pi \to N \times_{\rho_s} \Gamma$.
Similar to the homotopy exact sequence we make a equivalence relation of section as follows. If s, t are sections of a exact sequence

$$1 \to N \to \Pi \to \Gamma \to 1,$$

we say that s and t are equivalent sections, denoted by $s \equiv t$, if there exists $n \in N$ such that $ns(g)n^{-1} = t(g)$, for every $g \in \Gamma$. We denote by $\mathcal{S}_{\Pi\to\Gamma}$ the quotient set of sections under the equivalence relation $\equiv$. In particular, we have that $\mathcal{S}_{\pi_1^{\acute{e}t}(X|k,\overline{y})} = \mathcal{S}_{\pi_1^{\acute{e}t}(X,\overline{x})\to Gal_k}$. When we are working with a exact sequence of the form

$$1 \to N \to N \rtimes_\rho \Gamma \to \Gamma \to 1,$$

the set $\mathcal{S}_{N\rtimes_\rho\Gamma\to\Gamma}$ in addition to the above, is a pointed set with special element $[c]$, the canonical section of this exact sequence.

Definition 4.3.4. *Let N be a Γ-group, with structure homomorphism ρ. A continuous function $f : \Gamma \to N$ is called a* 1-***cocycle of*** *Γ with values in N if $f(gh) = \rho(g)f(h)$, for every $g, h \in \Gamma$. The set of 1-cocycles of Γ with values in N is denoted by $C^1(\Gamma, N)$.*

Let N be a Γ-group with structure homomorphism ρ. We said that $f_1, f_2 \in C^1(\Gamma, N)$ are **cohomologous**, denoted by $f_1 \sim f_2$, if there exists $n \in N$, such that $cf_1(\sigma) = f_2(\sigma)\rho_\sigma(c)$.

Definition 4.3.5. *Let N be a Γ-group. The* ***first non-abelian cohomology*** *of Γ with coefficients in N, denoted by $H^1(\Gamma, N)$ is the pointed set $(C^1(\Gamma, N)/\sim, [l])$, where $l : \Gamma \to N$ is the 1-cocycle such that $l(g) = 1$, for every $g \in \Gamma$.*

Let

$$1 \to N \to \quad \Pi \quad \to \Gamma \to 1, , \tag{4-1}$$

be a exact sequence, $f : \Gamma \to N$ be a continuous function and $s : \Gamma \to \Pi$, be a section of this exact sequence. We can twist s by f, defining

$$\begin{array}{rccl} s^f : \Gamma & \to & N \\ g & \mapsto & f(g)s(g), \end{array}$$

clearly, s^f is a set-theoretical section of the previous exact sequence, but not always a group-theoretical section, in other words, s^f is not always a group homomorphism.

$$\begin{aligned} s^f \text{ is a group homomorphism} &\Leftrightarrow s^f(g_1g_2) = s^f(g_1)s^f(g_2), \text{ for all } g_1, g_2 \in \Gamma \\ &\Leftrightarrow f(g_1g_2)s(g_1g_2) = f(g_1)s(g_1)f(g_2)s(g_2), \text{ for all } g_1, g_2 \in \Gamma \\ &\Leftrightarrow f(g_1g_2)s(g_1) = f(g_1)s(g_1)f(g_2), \text{ for all } g_1, g_2 \in \Gamma \\ &\Leftrightarrow f(g_1g_2) = f(g_1)s(g_1)f(g_2)s(g_1)^{-1}, \text{ for all } g_1, g_2 \in \Gamma \\ &\Leftrightarrow f(g_1g_2) = f(g_1)\rho_{g_1}(f(g_2)), \text{ for all } g_1, g_2 \in \Gamma \end{aligned}$$

Thus, s^f is a group homomorphism if, and only if f is a 1-cocycle (with the Γ-structure on N giving by ρ_s). Now we have a connection between sections of a exact sequence and 1-cocycles, we will explore this relation. Let s be a section of (3.1) and ρ^s the associated structure homomorphism, of N as a Γ-group, associated to s and $f_1, f_2 \in C^1(\Gamma, N)$

$$\begin{aligned} f_1, f_2 \text{ are cohomologous} &\Leftrightarrow \exists_{n\in N}\forall_{g\in\Gamma}\ (nf_1(g) = f_2(g)\rho^s_g(n)) \\ &\Leftrightarrow \exists_{n\in N}\forall_{g\in\Gamma}\ (nf_1(g) = f_2(g)s(g)ns(g)^{-1}) \\ &\Leftrightarrow \exists_{n\in N}\forall_{g\in\Gamma}\ (nf_1(g)s(g) = f_2(g)s(g)n) \\ &\Leftrightarrow \exists_{n\in N}\forall_{g\in\Gamma}\ (ns^{f_1}(g) = s^{f_2}(g)n) \\ &\Leftrightarrow \exists_{n\in N}\forall_{g\in\Gamma}\ (ns^{f_1}(g)n^{-1} = s^{f_2}(g)) \\ &\Leftrightarrow s^{f_1},\ s^{f_2} \text{ are equivalent sections.} \end{aligned}$$

Thus, fixing a section s of (3.1), the next function is well defined

$$\begin{aligned} \_^f : H^1(\Gamma, N) &\to \mathcal{S}_{\Pi\to\Gamma} \\ [f] &\mapsto \left[s^f\right], \end{aligned}$$

and moreover, the previous argument show that is an injective function. If $[t] \in \mathcal{S}_{\Pi\to\Gamma}$, let

$$\begin{aligned} \delta(s,t) : \Gamma &\to N \\ g &\mapsto t(g)s(g)^{-1}, \end{aligned}$$

clearly f is a continuous function, satisfying that $s^f = t$, and as we seen before this implies that $f \in C^1(\Gamma, N)$. Furthermore this argument now shows that $\_^f$ is bijective. In other words, we can back-and-forth between sections of an exact sequence and cohomology classes of 1-cocycles. Note that this is not a canonical isomorphism, because it depends on the chosen section. Next we need to use use the inverse map of $\_^f$, briefly we will describe them. Fixing a section s of (3.1), for every section t of (3.1), consider the 1-cocycle $\delta(s,t) : \Gamma \to N$ defined as above and the inverse map is then defined by

$$\begin{aligned} \delta(s, \_) : \mathcal{S}_{\Pi\to\Gamma} &\to H^1(\Gamma, N) \\ [t] &\mapsto [\delta(s,t)], \end{aligned}$$

Then, $\delta(s, \_)$ is the inverse function of $\_^f$, and $\delta(s,t)$ is called the difference cocycle of the sections s and t. Again, we know that $\mathcal{S}_{\Pi\to\Gamma}$ and $H^1(\Gamma, N)$ are in bijection, but this is not a natural bijection, because it is depends on the section chosen. But, in the case of a exact sequence of the form

$$1 \to N \to N \rtimes_\rho \Gamma \to \Gamma \to 1,$$

thush, it is possible to define a natural bijection given by the canonical split of this sequence and the trivial cohomology class on coclycles on the other hand. Now we introduce a special class of torsors in order to give other classification of sections, or equivalently, cohomology classes of 1-cocycles.

Definition 4.3.6. *Let N be a Γ-group. A Γ-**equivariant right** N-**torsor** is a profinite space P with a continuous left action of Γ and a right continuous, free and transitive Γ-equivariant action of N.*

Fixing a section s of (3.1), the every torsor P gives a twist of this section, similarly as the case of 1-cocycles. Let P be a Γ-equivariant right N-torsor (N has the Γ-structure induced by the section s) and $q \in P$. Recall that every element of Π can be written in a unique way as $ns(g)$, for some $n \in N$ and $g \in \Gamma$. Define the next continuous action

$$\begin{array}{rcl} P \times \Pi & \to & P \\ (p, ns(g)) & \mapsto & g^{-1}pn, \end{array}$$

then, the stabilizer of q of this action is

$$Stab(q) = \{ns(g) \in \Pi | qn = gq\},$$

let $j : \Pi \to \Gamma$ be the homomorphism appearing in (3.1). $j|_{Stab(q)}$ is an isomorphism onto Γ. Indeed, is $g \in \Gamma$, then $s(g) \in \Pi$ is a preimage of g, then j is surjective and

$$\begin{array}{rcl} ns(g) \in ker(j) \cap Stab(q) & \Leftrightarrow & j(ns(g)) = 1 \text{ and } qn = gq \\ & \Leftrightarrow & j(n)j(s(g)) = 1 \text{ and } qn = gq \\ & \Leftrightarrow & g = 1 \text{ and } gn = gq \\ & \Leftrightarrow & g = 1 \text{ and } n = gq \\ & \Leftrightarrow & g = 1 \text{ and } g = 1, \end{array}$$

the last equivalence is true since the action of N in P is transitive. Therefore $j|_{Stab(q)}$ is an isomorphism, let $s^{P,q}$ be the inverse homomorphism of $j|_{Stab(q)}$. If we redefine the target group by $s^{P,q} : \Gamma \to \Pi$, then $s^{P,q}$ is a section of j. $s^{P,q}$ depends on P and q, but it equivalence class does not depends on q, if $r \in P$, since the action of N on P is transitive, we have that there exists $n \in N$ such that $q.n = r$, thus $Stab(q) = nStab(r)n^{-1}$ and therefore $s^{P,q} = ns^{P,r}n^{-1}$, in other words $[s^{P,q}] = [s^{P,r}]$. Then the class of a section constructed in this way, only dependes on P. Note that, this torsor gives rise to the 1-cocycle defined by $\delta(s, s^{P,q})$, since

the equivalence class of $s^{P,q}$ only depends on P, then the cohomological class of this $\delta(s, s^{P,q})$ only depends on P. Trivially, we have that

$$ {}_s\delta(s, s^{P,q}) = {}_s{}^{P,q}.$$

Let t be a section of

$$1 \to N \to \Pi \to \Gamma \to 1,$$

Consider the coset space

$$\Pi/t(\Gamma),$$

(the previous space is only considered as a topological group forgetting the natural group sctructure of this quotient). $\Pi/t(\Gamma)$ is naturally a right N-torsor with the right multiplication by an element of N, as the action defined in this set. The Γ-action on this set is defined by

$$\begin{array}{rcl} \Gamma \times \Pi/t(\Gamma) & \to & \Pi/t(\Gamma) \\ (g, pt(\Gamma)) & \mapsto & ps(g^{-1})t(\Gamma), \end{array}$$

with this action, is not difficult to prove that $\pi/t(\Gamma)$ is a Γ-equivariant right N-torsor. This torsor is called the difference torsor between s and t and we denoted by $\Delta(s,t)$, the pointed torsor $(\Pi/t(\Gamma), 1t(\Gamma))$. Using the action of Γ defined on the torsor $\Gamma/t(\Gamma)$ as before, we have in this case that

$$\begin{array}{rcl} ns(g) \in Stab(1) & \Leftrightarrow & 1t(\Gamma).n = g.1t(\Gamma) \\ & \Leftrightarrow & nt(\Gamma) = 1.s(g^{-1})t(\Gamma) \\ & \Leftrightarrow & ns(g) \in t(\Gamma), \end{array}$$

then, if $ns(g) \in Stab(1)$, there exists $g^{'} \in \Gamma$, such that $ns(g) = t(g^{'})$, aplying j of the both sides of this equation we obtain that $g = g^{'}$, and thus $(t \circ j)(ns(g)) = ns(g)$, or equivalently t is a inverse for $j|_{Stab(1t(\Gamma))}$, in other words, $t = s^{\Delta(t,s)}$. The homomorphism

$$\begin{array}{rcl} \varphi : \Pi & \to & N \\ g & \mapsto & gt(j(g^{-1})), \end{array}$$

Is surjective and is kernel is $t(\Gamma)$, in particular, as a set $\Pi/t(\Gamma)$ is in bijection with N, but this is not an isomorphism of Γ-equivariant right N-torsors. The equivaelence of sections are reflected as a isomorphism of torsor, to be precise, $\Pi/t(\Gamma) \simeq N$ as Γ-equivariant right N-torsors if, and only if s and t are equivalent sections.
Then we have equivalences between N-conjugacy clases of sections, cohomology clases of 1-cocycles and Γ-equivariant right N-torsors. The next proposition summarize the results proved previously.

Proposition 4.3.4. *Let N be a Γ-group and $\rho : \Gamma \to Aut(N)$ be the structure homomorphism.*

(i) There exists a natural bijection between the pointed sets $\mathcal{S}_{N\rtimes_\rho\Gamma\to\Gamma}$, $H^1(\Gamma,N)$ *and* $Tors_\Gamma(N)$.

(ii) After fixing a section s *of a exact sequence*

$$1\to N\to\Pi\to\Gamma\to 1,$$

there exists bijections between the sets $\mathcal{S}_{\Pi\to\Gamma}$, $H^1(\Gamma,N)$ *and* $Tors_\Gamma(N)$, *given by*

$$\delta(s,\_):\mathcal{S}_{\Pi\to\Gamma}\to H^1(\Gamma,N),$$

and

$$\Delta(s,\_):\mathcal{S}_{\Pi\to\Gamma}\to Tor_N(\Gamma).$$

Then, if we want to study Grothendieck's section conjecture we can replace the set of equivalence classes of sections by cohomology or torsors. In the prove of the next theorem we give an example of the use of this relation. We start with a few definitions.

Definition 4.3.7. *Let* Γ *be a profinite group. The* ***abelianization*** *of* Γ, *denoted by* Γ^{ab}, *is the quotient of* Γ *by the closure of its commutator subgroup. The natural quotient map* $\Gamma\to\Gamma^{ab}$ *is called* ***abelianization map****.*

For a scheme Y and a geometric point $\overline{y}$ of Y, we denote by $\pi^{ab}(Y,\overline{y})$ the abelianization of $\pi_1^{\acute{e}t}(Y,\overline{y})$.
Let k be a field and X be a compact and geometrically integral k-scheme. The abelianization map

$$f:\pi_1^{\acute{e}t}(X_{\overline{k}},\overline{x})\to\pi_1^{ab}(X,\overline{x})$$

induces a abelianization of the homotopy exact sequence associated to X. Inded, let Π be the group given by the pushout of the next diagram of groups

$$\begin{array}{ccc}\pi_1^{\acute{e}t}(X_{\overline{k}},\overline{x}) & \longrightarrow & \pi^{\acute{e}t}(X,\overline{x})\\ {\scriptstyle f}\downarrow & & \\ \pi_1^{ab}(X,\overline{x}) & & \end{array}$$

the group Π fits in a exact sequence

$$1\to\pi_1^{ab}(X_{\overline{k}},\overline{x})\to\Pi\to Gal_k\to 1,$$

we refer to this section as the **abelianized homotopy exact sequence** and sometimes we denote them by $\pi_1^{ab}(X|k)$. Moreover, the next diagram is commutative

$$\begin{array}{ccccccccc}1 & \longrightarrow & \pi_1^{\acute{e}t}(X_{\overline{k}},\overline{x}) & \longrightarrow & \pi_1^{\acute{e}t}(X,\overline{x}) & \longrightarrow & Gal_k & \longrightarrow & 1\\ & & {\scriptstyle f}\downarrow & & {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & \pi_1^{ab}(X_{\overline{k}},\overline{x}) & \longrightarrow & \Pi & \longrightarrow & Gal_k & \longrightarrow & 1\end{array}$$

where $g : \pi_1^{\acute{e}t}(X, \overline{x}) \to \Pi$ is the homomorphism given by pushout. If $s : Gal_k \to \pi_1^{\acute{e}t}(X, \overline{x})$ is a section of the homotopy exact sequence, then $g \circ s$ is a section of the abelianized homotopy exact sequence. This section is called the **abelianization** of s, or more precisely, the well-defined map

$$\begin{array}{rcl} ab : \mathcal{S}_{\pi_1^{\acute{e}t}(X|k)} & \to & \mathcal{S}_{\Pi \to Gal_k} \\ [s] & \mapsto & [g \circ s], \end{array}$$

is called the **abelianization map of sections**.

Theorem 4.3.1. ***(Injectivity of the section conjecture)*** *Let X be a smooth, projective k- curve or genus at least 2 , where k finitely generated over $\mathbb{Q}$. The profinite Kummer map κ_X of X is injective.*

Grothendieck known that the profinite kummer map κ_X is injective, we give an sketch of the proof that involves some techniques of abelian varieties. Let $x \in X(k)$ be a rational point of X and let s_x be the sections associated to x. For all $m \in \mathbb{Z}^+$, define

$$\begin{array}{rcl} F_m : X(k) & \to & H^1(Gal_k, \pi_1^{ab}(X_{\overline{k}}, \overline{x})/m\pi_1^{ab}(X_{\overline{k}}, \overline{x})) \\ y & \mapsto & j_m \circ \delta(ab(s_x), ab(s_y)), \end{array}$$

where $j_m : \pi_1^{ab}(X_{\overline{k}}, \overline{x}) \to \pi_1^{ab}(X_{\overline{k}}, \overline{x})/m\pi_1^{ab}(X_{\overline{k}}, \overline{x})$ is the canonical quotient homomorphism. Let J be the jacobian of X, by a theorem due to Serre and Lang (See for example [49]), we have that

$$\pi_1^{ab}(X_{\overline{k}}, \overline{x})/m\pi_1^{ab}(X_{\overline{k}}, \overline{x}) \simeq (J_{\overline{k}})_m$$

where, $(J_{\overline{k}})_m$ is the m-torsion subgroup of the abelian variety $J_{\overline{k}}$. Then we can redefine the map F_m under this isomorphism to

$$F_m : X(k) \to H^1(Gal_k, (J_{\overline{k}})_m),$$

by linearity, F_m induces a map

$$G_m : Div^0(X) \to H^1(Gal_k, (J_{\overline{k}})_m),$$

where $Div^0(X)$ is the group of divisors of degree 0 of X. From the canonical morphism $X \to J$, we get a map $H : Div^0(X) \to J(k)$. Let $j : Spec(\overline{k}) \to Spec(k)$ be the scheme morphism induced by the canonical inclusion $k \hookrightarrow \overline{k}$, then the map

$$\begin{array}{rcl} j^* : J(k) & \to & J(\overline{k}) \\ f & \to & f \circ j, \end{array}$$

is a injective function and its image is

$$J(\overline{k})^{Gal_k} := \{f \in J(\overline{k}) | f \circ \sigma = f, \text{ for all } \sigma \in Gal_k\}.$$

On the other hand, the

$$k_m : J(\overline{k})^{Gal_k} \quad \rightarrow \quad H^1(Gal_k, (J_{\overline{k}})_m),$$

coming from a Kummer sequence, fits in the commutative diagram

$$\begin{array}{ccc} Div^0(X) & \xrightarrow{G_m} & H^1(Gal_k, (J_{\overline{k}})_m) \\ \Big\downarrow H & & \Big\uparrow k_m \\ J(k) & \xrightarrow[j^*]{} & J(\overline{k})^{Gal_k} \end{array}$$

Let y be a k-rational point of X, such that $\kappa_X(x) = \kappa_X(y)$, in particular, for all $m \in \mathbb{Z}^+$ $G_m(x-y) = 0$, then $k_m \circ j^* \circ H(x-y) = 0$, equivalent, $j^* \circ H(x-y) \in \cap_{m\in\mathbb{Z}^+} ker(k_m)$, thus $j^* \circ H(x-y)$ is divisible in $J(k)$.

Theorem 4.3.2. ***(Mordell-Wéil-Lang-Nerón theorem)*** *If k is a field finitely generated over $\mathbb{Q}$ and A is an abelian variety, then the set $A(k)$ is finitely generated group.*

The previous theorem (whose proof can be consulted in [Lang] Chapter I corollary 4.3) implies that the subgroup of divisible elements in $J(k)$ is trivial, therefore, $j^* \circ H(x-y) = 0$, but j^* is bijective and H is injective, then $x - y = 0$ as degree 0 divisors, since X has positive genus, then we can conclude that $x = y$. This completes the prove of the injectivity of κ_X. Thereby, Grothendieck's section conjecture is the surjectivity of the profinite Kummer map. There is not too much known about this conjecture, it seems that, at the moment, it is far from being proved. Deligne suggest to Grothendieck a conjecturally relation of the section conjecture and Mordell's conjecture/Falting's theorem, that states for a curve C defined a number field k, the set k-rational point of C is finite. This relation was suggest to Grothendieck by Deligne, who thinks that he gave a proof of that the section conjecture implies Mordell's conjecture, however, he find a gaps in his prove a gap that, at the moment, is not filled and no other proof are given.

Bibliography

[1] Balakrishnan, J. S., Dan-Cohen, I., Kim, M., Wewers, S. (2018). A non-abelian conjecture of Tateâ€“Shafarevich type for hyperbolic curves. Mathematische Annalen, 372(1-2), 369-428.

[2] Bombieri, E. (1990). The Mordell conjecture revisited. Annali della Scuola Normale Superiore di Pisa-Classe di Scienze, 17(4), 615-640.

[3] Deligne, P. (1980). La conjecture de Weil: II. Publications Mathématiques de l'IHéS, 52, 137-252.

[4] Esnault, H., Hai, P. H. (2008). Packets in Grothendieck's section conjecture. Advances in Mathematics, 218(2), 395-416.

[5] Girondo, E., GonzÃ¡lez-Diez, G. (2012). Introduction to compact Riemann surfaces and dessins d'enfants (Vol. 79). Cambridge University Press.

[6] Grothendieck, A. (1958, August). The cohomology theory of abstract algebraic varieties. In Proceedings of the International Congress of Mathematicians (pp. 1)

[7] Grothendieck, A. (1983). Letter to Faltings. Geometric Galois Actions, 1.

[8] Grothendieck, A. (1997). Sketch of a Programme. Lond. Math. Soc. Lect. Note Ser, 242, 243-283.

[9] Grothendieck, A., Raynaud, M. (2002). Revêtements étales et groupe fondamental (SGA 1). arXiv preprint math/0206203.

[10] Hartshorne, R. (2013). Algebraic geometry (Vol. 52). Springer Science Business Media.

[11] Hatcher, A. (2002). Algebraic Topology. Cambridge University Press.

[12] Ihara, Y. (1997). Some illustrative examples for anabelian geometry in high dimensions. London Math. Soc. Lect. Note Ser., 1, 127-138.

[13] Jacobson, N. (1964). Lectures In Abstract Algebra; Volume 3: Theory Of Fields And Galois Theory.

[14] Koenigsmann, J. (2005). On the section conjecture in anabelian geometry. Journal fur die reine und angewandte Mathematik, 2005(588), 221-235.

[15] Kock, B. (2001). Belyi's theorem revisited. arXiv preprint math/0108222.

[16] Landesman, A. (2020). Invariance of the fundamental group under base change between algebraically closed fields. arXiv preprint arXiv:2005.09690.

[17] Lenstra, H. (2003). Profinite groups. Lecture notes available on the web.

[18] McLarty, C. (2007). The Rising Sea: Grothendieck on simplicity and generality. na.

[19] MAEHARA, K. (2001). Conjectures on birational geometry. The Academic Reports, the Faculty of Engineering, Tokyo Polytechnic University, 24(1), 9-18.

[20] Murre, J. P., Anantharaman, S. (1967). Lectures on an introduction to Grothendieck's theory of the fundamental group. Bombay: Tata Institute of Fundamental Research.

[21] Marcus, D. A., Sacco, E. (1977). Number fields (Vol. 2). New York: Springer.

[22] Milne, J. S. (2009). Algebraic number theory (v3. 07).

[23] Milne, JS (1997). Class field theory. reading notes available at http: // www. math. lsa. umich. edu / jmilne .

[24] Milne, J. S. (1998). Lectures on étale cohomology. Available on-line at http://www. jmilne. org/math/CourseNotes/LEC. pdf.

[25] Milne, J. S., Milne, J. S. (1980). Etale cohomology (PMS-33) (Vol. 5657). Princeton university press.

[26] Mochizuki, S. (1996). The profinite Grothendieck conjecture for closed hyperbolic curves over number fields. Journal of Mathematical Sciences-University of Tokyo, 3(3), 571-628.

[27] Mochizuki, S. (1999). The local pro-p anabelian geometry of curves. Inventiones mathematicae, 138(2), 319-423.

[28] Mochizuki, S. (2002). The absolute anabelian geometry of canonical curves. Kyoto University. Research Institute for Mathematical Sciences [RIMS].

[29] Mochizuki, S. (2003). Topics surrounding the anabelian geometry of hyperbolic curves. Galois groups and fundamental groups, Math. Sci. Res. Inst. Publ, 41, 119-165.

[30] Mochizuki, S. (2008). Topics in Absolute Anabelian Geometry: Generalities. I. Kyoto University, Research Institute for Mathematical Sciences.

[31] Mochizuki, S. (2013). Topics in absolute anabelian geometry II: decomposition groups and endomorphisms. J. Math. Sci. Univ. Tokyo, 20(2), 171-269.

[32] Mochizuki, S. (2015). Topics in absolute anabelian geometry III: global reconstruction algorithms. J. Math. Sci. Univ. Tokyo, 22(4), 939-1156.

[33] Nakamura, H. (1990). Galois rigidity of the étale fundamental groups of punctured projective lines. J. reine angew. Math, 411, 205-216.

[34] Nakamura, H. (1994). Galois rigidity of pure sphere braid groups and profinite calculus. J. Math. Sci. Univ. Tokyo, 1(1), 71-136.

[35] Nakamura, H. (1997). Galois rigidity of profinite fundamental groups. Sugaku Expositions, 10(2).

[36] Nakamura, H., Tamagawa, A., Mochizuki, S. (2001). The conjecture on the fundamental groups of algebraic curves. Sugaku Expositions, 14(1), 31-54.

[37] Neukirch, J., Schmidt, A., Wingberg, K. (2013). Cohomology of number fields (Vol. 323). Springer Science Business Media.

[38] Neukirch, J. (2013). Algebraic number theory (Vol. 322). Springer Science Business Media.

[39] Neukirch, J. (1986). Class field theory (Vol. 280). Berlin: Springer.

[40] Oort, F. (1997). The algebraic fundamental group. LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES, 67-84.

[41] Poonen, B. (2017). Rational points on varieties (Vol. 186). American Mathematical Soc.

[42] Pop, F. (1990). On the Galois theory of function fields of one variable over number fields. J. reine angew. Math, 406, 200-218.

[43] Pop, F. (1994). On Grothendieck's conjecture of birational anabelian geometry. Annals of Mathematics, 139(1), 145-182. Pop 4 Pop, F. (1997). Glimpses of Grothendieck's anabelian geometry. London Mathematical Society Lecture Note Series, 113-126.

[44] Pop, F. (2005). Anabelian Phenomena in Geometry and Arithmetic. Lecture Notes of the AWS.

[45] Pop, F. (2010). On the birational p-adic section conjecture. Compositio Mathematica, 146(3), 621-637.

[46] Saidi, M. (2010). Good sections of arithmetic fundamental groups. arXiv preprint arXiv:1010.1313.

[47] Saidi, M. (2011). Around the Grothendieck anabelian section conjecture. Non-abelian Fundamental Groups and Iwasawa Theory, 393, 72.

[48] Szamuely, T. (2009). Galois groups and fundamental groups (Vol. 117). Cambridge University Press.

[49] Szamuely, T. (2012). Heidelberg lectures on fundamental groups. In The Arithmetic of Fundamental Groups (pp. 53-74). Springer, Berlin, Heidelberg.

[50] Schneps, L., Lochak, P. (Eds.). (1997). Geometric Galois actions: around Grothendieck's esquisse d'un programme. Cambridge University Press.

[51] Serre, J. P. (2016). Topics in Galois theory. AK Peters/CRC Press.

[52] Silverman, J. H. (2009). The arithmetic of elliptic curves (Vol. 106). Springer Science Business Media.

[53] Stix, J. (2011). The Brauer Manin obstruction for sections of the fundamental group. Journal of Pure and Applied Algebra, 215(6), 1371-1397.

[54] Stix, J. (2012). Rational points and arithmetic of fundamental groups: Evidence for the section conjecture (Vol. 2054). Springer.

[55] Tamagawa, A. (1997). The Grothendieck conjecture for affine curves. Compositio Mathematica, 109(2), 135-194.

[56] Uchida, K. (1976). Isomorphisms of Galois groups. Journal of the Mathematical Society of Japan, 28(4), 617-620.

[57] Uchida, K. (1977). Isomorphisms of Galois groups of algebraic function fields. Annals of Mathematics, 106(3), 589-598.

[58] Uchida, K. (1981). Homomorphisms of Galois groups of solvably closed Galois extensions. Journal of the Mathematical Society of Japan, 33(4), 595-604.

[59] Uchida, K. (1982). Galois groups of unramified solvable extensions. Tohoku Mathematical Journal, Second Series, 34(2), 311-317.

[60] Voevodsky, V. A. (1991). Galois representations connected with hyperbolic curves. Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya, 55(6), 1331-1342.