Indian Institute of Technology, Guwahati

Bachelor's Thesis | EE498

Generalized Galois Theories & Classical Algebraic Geometry

Animesh Renanse
180108048

April 18, 2022

CERTIFICATE

This is to certify that the work contained in this project report entitled "Generalized Galois Theories - I" submitted by Animesh Renanse (Roll No. 180108048) to the Department of Electronics & Electrical Engineering, Indian Institute of Technology Guwahati towards partial requirement of Bachelor of Technology in Electronics & Electrical Engineering has been carried out by him under my supervision.

It is also certified that this report is a survey work based on the references in the bibliography written in his own words and understanding. There is no claim of new results.

Turnitin Similarity: 21 %

Guwahati - 781 039
November 2021

Prof. Rupam Barman
Project Supervisor

ABSTRACT

Let K be a field and $L \supseteq K$ be a finite dimensional Galois extension. The fundamental theorem of Galois theory establishes an isomorphism between lattice of subgroups of the Galois group and the dual lattice of intermediate field extensions of $L \supseteq K$. This result is usually used to show the insolvability of 5^{th} order general polynomials by radicals. However, the main ideas of Galois theory of studying an object by it's group of symmetries runs much deeper than this. In the previous century, this main idea has been taken up by a lot of people to study much more general theories than the traditional Galois theory over fields, for example, around the mid of the previous century, mathematicians started seeing certain *Galoisian* relation between factorizations of covering space and it's group of *deck*-transformations. This resulted in what is now called Galois theory of schemes, which is hallmark of modern algebraic geometry. On the other side of the spectrum, there have been applications of Galois theory in theoretical computer science, especially in theoretical understanding of *Programs, Algorithms & Functions*. We discuss this more in detail in the introduction.

Motivated both by pure mathematical and computer science applications, the present text explores the technicalities of various Galois theories, from it's roots in field theory and Abel-Ruffini theorem, Grothendieck Galois theory for commutative algebras, it's generalization to arbitrary dimensional algebras, to the setting of more abstract categorical Galois theorem of Janelidze, proving almost all of the theorems along the way. However, for the latter, we restrict ourselves only to introduce the main terminologies and primary results therein and we hope to establish the categorical Galois theorem in the next phase of this project.

This text is expository in nature and no new result is being claimed.

Introduction & Motivation

Let $[L : K]$ denote a finite dimensional Galois extension of fields. The fundamental theorem of Galois theory establishes an isomorphism between the lattice of subgroups of the Galois group of $[L : K]$ and the dual lattice of intermediate field extensions (Theorem 3). This forms a way to transfer group theoretic information to field theoretic information and vice-versa. A particular application of this result is that of insolvability of the 5^{th} order general polynomial (Corollary 1.7.11).

This is usually where the story of classical Galois theory ends, but one can go further. A field is usually a very restrictive structure, and a field extension L over K can be treated as a K-algebra L[1]. This leads to a natural question : "*Does the fundamental theorem holds for K-algebras?*". The question, as stated is inherently vague; there's no notion right now of concepts like "extensions of algebras" and their "Galois group". But this abstraction doesn't have to be quite so literal. What we will see in the Section 2 would indeed be a generalization of classical Galois theory over fields to over commutative algebras (that is, the fundamental theorem in the latter case will imply the fundamental theorem in the former), but the generalization here leads to a theorem which doesn't necessarily introduces literal abstractions of the concept of "extensions" and of "Galois groups" to K-algebras, but rather talks about the interaction between a Galois extension of the field K, say $[L : K]$, and those K-algebras split by L. In particular, the fundamental theorem in this case will tell us that all such finite dimensional K-algebras (split by L) are in a sense (categorical sense) are equivalent to all those finite sets which admits an action of the Galois group of $[L : K]$ (Theorem 7). This is a *stripped* down version of much bigger Grothendieck's Galois theory of schemes[2].

However, there's more room to improve. In both the discussions, we saw finite dimensionality in the background. In the case of fields, we demand field extensions be finite dimensional. In the case of commutative algebras, we demand field extensions and algebras be finite dimensional. But one can imagine what can go wrong when we try to hastily generalize the Grothendieck's theory over commutative algebras to the infinite dimensional case. One can think that a K-algebra A might be given as a union of all of it's finite dimensional subalgebras. This is actually true, under some more mild hypotheses, as shown in Proposition 3.2.11 of the main text. Note that an arbitrary dimensional Galois extension L over K is also a K-algebra satisfying the above hypotheses, and thus is a union of all finite-dimensional Galois *sub*-extensions over K. Motivated by this, one can thus heuristically argue that if we take colimit everywhere in fundamental theorem of Grothendieck's Galois theory, and let the allowed collection to grow larger if required (it might not happen that any given category would be closed under colimits), then we can hope to get an arbitrary dimensional version of Grothendieck's Galois theory. Working out the details of this heuristic idea is the goal of Section 3, where we see that this indeed becomes true, however will require a certain bit of newer

[1]Remember a K-algebra is a K-vector space with a multiplication on it which remains compatible with scalar product.

[2]The more complete picture of Galois theory will hopefully come in the next phase of the project, where we will discuss covering spaces.

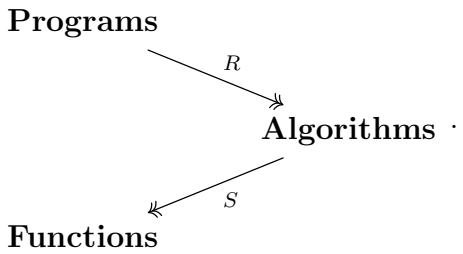
terminology. This culminates in Theorem 9.

The sequence of generalizations discussed above generally follows that from concrete objects (like fields) to something more abstract (finite/arbitrary dimensional commutative algebras). The next natural step must then be commutative rings. While a theory of Galois theory over commutative rings does exist due to A.R. Magid and it generalizes all the previous ones discussed so far, we do not introduce it in this order. We will instead introduce an even more general Galois theory, which will be purely based on categories, called categorical Galois theory of Janelidze, as in [Jan89] & [Jan91]. The reason being that this general theory generalizes the one over commutative rings quite nicely and thus gives a nice example to understand it, as it is indeed quite abstract. However, we end the phase I of this project just after introducing the terminology used in categorical Galois theory and some of the basic results derived from it. We will pick up in the phase II and will prove the categorical Galois theorem and study as its example the Galois theory of commutative rings and then further go to covering spaces.

One can say that the main idea of Galois theory is that of studying an object by the group of it's symmetries. This is nicely explained in the following use of Galois theory in computer science by [Yan14]. **This example further motivates the importance and relevance of studying more abstract generalizations of Galois theory, as undertaken in the present text.**

An example of classical Galois theory in computer science

There is a hierarchy of how one gets from a **Program** to an **Algorithm** and finally to a **Function**. For example, consider the function `sort` which sorts a string according to order. This is in the hierarchy of Function as it only describes what the function does; it takes a list of integers and gives back the same list of integers but in a monotonic order. A sorting algorithm, like `mergesort` sits in the hierarchy of Algorithms as it *describes* one way (out of countable many) to achieve the function `sort`. Note that there are many other algorithms which achieves the function of `sort`, like `bubblesort`, `quicksort` etc. Finally, we have various implementations of algorithm `mergesort`, say $\texttt{mergesort}_a$ and $\texttt{mergesort}_b$ both of which lives in the hierarchy of Programs/Descriptions. The following diagram summarizes the above discussion:



This diagram thus tells us that the set of all algorithms sits in the middle of that of programs and functions. In fact, more is true. First of all, the above three sets have more structure; they are graphs, and second that the surjective maps as above are graph homomorphisms which fixes objects. We will see that certain subgroups of those automorphisms of programs which fixes algorithms are in bijection with intermediate algorithm universes. We now make this precise by introducing the language which formalizes the building blocks of algorithms, the primitive recursive functions:

Recall that a primitive recursive function (PRF) is one that is "recursively" defined by the following "atomic" PRFs:

- (*Constant zero*) $z : \mathbb{N}^0 \to \mathbb{N}$ is a PRF.
- (*Successor*) $s : \mathbb{N} \to \mathbb{N}$ which takes $x \mapsto x + 1$ is a PRF.
- (*Projection*) $p_i^n : \mathbb{N}^n \to \mathbb{N}$ which takes $(x_1, \ldots, x_i, \ldots, x_n) \mapsto x_i$ is a PRF.

and these atomic PRFs are composed by the following operation

- (*Composition*) Let $f : \mathbb{N}^n \to N$ and $g_1, \ldots, g_n : \mathbb{N}^m \to \mathbb{N}$ be a PRF. Then the following $h : \mathbb{N}^m \to \mathbb{N}$ is a PRF:

$$\begin{aligned} h : \mathbb{N}^m &\longrightarrow \mathbb{N} \\ (x_1, \ldots, x_m) &\longmapsto f\left(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m)\right). \end{aligned}$$

and finally the following is also defined to be a PRF:

- Let $f : \mathbb{N}^n \to \mathbb{N}$ and $g : \mathbb{N}^{n+2} \to \mathbb{N}$ be PRFs. Then the function defined as follows is a PRF:

$$\begin{aligned} h : \mathbb{N}^{n+1} &\longrightarrow \mathbb{N} \\ (\kappa, x_1, \ldots, x_n) &\longmapsto \begin{cases} f(x_1, \ldots, x_n) & \text{if } \kappa = 0 \\ g(y, h(y, x_1, \ldots, x_n), x_1, \ldots, x_n) & \text{if } \kappa = s(y). \end{cases} \end{aligned}$$

One can similarly extend the above definition to that of PRFs with target $\mathbb{N}^i$ for $i > 0$.
With the definition of PRFs in motion, we now define the collection of all descriptions/programs of PRFs as the graph **PRdesc** which has as objects all powers $\mathbb{N}^n$ for $n \geq 0$ and arrows $p : \mathbb{N}^n \to \mathbb{N}^m$ as programs of PRFs between them. We next define the graph of functions **PRfunc** which has objects all powers $\mathbb{N}^n$ for $n \geq 0$ and arrows $f : \mathbb{N}^n \to \mathbb{N}^m$ are all PRFs between them. Clearly, there is a graph surjection

$$Q : \textbf{PRdesc} \twoheadrightarrow \textbf{PRfunc}$$

which is identity on objects but take each program to the function it describes. Clearly, **PRfunc** = **PRdesc**/ $\sim$ where $p, q : \mathbb{N}^a \to \mathbb{N}^b$ in **PRdesc** are related when they define the same function:

$$p \sim q \iff Q(p) = Q(q).$$

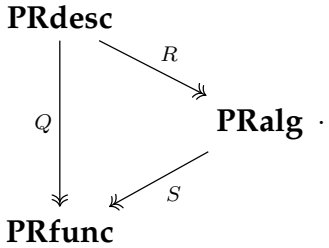
This motivates the definition of that of an automorphism of **PRdesc** as follows:

$$\begin{aligned} \phi : \textbf{PRdesc} &\longrightarrow \textbf{PRdesc} \\ p &\longmapsto \phi(p) \end{aligned}$$

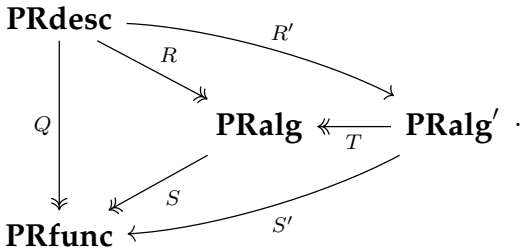
where $Q(\phi(p)) = Q(p)$, that is, ϕ is defined an automorphism when it maps each program to a program which implements the same function. Clearly, collection of all such automorphisms of **PRdesc** forms a group, called the Galois group of **PRdesc** over **PRfunc** and is denoted:

$$\textbf{Gal}\,[\textbf{PRdesc} : \textbf{PRfunc}].$$

We next define the intermediary where algorithms resides, the *primitive recursive algorithmic universe*, **PRalg**. This is a graph with objects as powers of $\mathbb{N}$ and which is quotient of **PRfunc** and it's quotient is **PRdesc**. More precisely, we require two surjective graph homomorphisms R and S which makes the following diagram commute:



Note that this looks much closer to the heuristic diagram we drew on the previous page. We then simply define a *primitive recursive quotient algorithmic universe*, $\mathbf{PRalg}'$ as a primitive recursive algorithmic universe which further has a surjective graph homomorphism which makes the following diagram commute:



The collection of all quotient universes forms a poset where $\mathbf{PRalg}'_1 \leq \mathbf{PRalg}'_2$ if and only if there exists $T : \mathbf{PRalg}'_2 \twoheadrightarrow \mathbf{PRalg}'_1$, that is, only if $\mathbf{PRalg}'_1$ is a quotient of $\mathbf{PRalg}'_2$. We denote this poset by **UNIV**. In a similar fashion we denote the poset of all subgroups of $\mathbf{Gal}\,[\mathbf{PRdesc} : \mathbf{PRfunc}]$ as **SGRPS**.
We finally have the following fundamental theorem, akin to fundamental theorem of Galois theory:

Theorem : (*The Fundamental Theorem, [Yan14]*) Consider the following map:

$$\begin{aligned} \Psi : \mathbf{SGRPS} &\longrightarrow \mathbf{UNIV} \\ G &\longmapsto \Psi(G) := \mathbf{PRdesc}/\sim_G \end{aligned}$$

where, for $p, q : \mathbb{N}^a \to \mathbb{N}^b$ in **PRdesc**, we define $p \sim_G q \iff \exists \phi \in G$ such that $\phi(p) = q$. This is an equivalence relation. Conversely, we define the following map:

$$\begin{aligned} \Phi : \mathbf{UNIV} &\longleftarrow \mathbf{SGRPS} \\ \mathbf{PRalg}' &\longmapsto \Phi(\mathbf{PRalg}') \end{aligned}$$

where $\Phi(\mathbf{PRalg}') := \left\{ f : \mathbf{PRdesc} \xrightarrow{\cong} \mathbf{PRdesc} \mid \forall p \in \mathbf{PRdesc},\ R'(p) = R'(f(p)) \right\}$. This is a subgroup of $\mathbf{Gal}\,[\mathbf{PRdesc} : \mathbf{PRfunc}]$. Define a sub-poset of **SGRPS**, called poset of restricted subgroups which is the sub-collection of only those subgroups for which $\Phi \circ \Psi(G) = G$. We denote this by $\mathbf{SGRPS}^{\text{rest}}$. Then, the maps

$$\Phi : \mathbf{UNIV} \rightleftarrows \mathbf{SGRPS}^{\text{rest}} : \Psi$$

defines an order reversing isomorphism of lattices, that is, $\Psi \vdash \Phi$ is a **Galois connection**.

What the above theorem tells us is that to study a particular algorithm, we can equivalently study the collection of all automorphisms of programs which sends a program to other program implementing the same algorithm. Moreover, this further formalizes the heuristic that says that:

"An algorithm doesn't depend on the program which you choose to implement it!"

This shows the actual power of just the classical Galois theory in situations arising in study of algorithms. The story doesn't ends here. The paper [Yan14] further discusses the homotopy theoretic perspective on the constructions defined above, in particular, from the view of covering spaces and deck-transformations. We omit the discussion of the latter theme here, but will revisit them in the phase II of this thesis.

The above discussion hopefully gives a good justification from an application point of view of Galois theory. In this project, we engage in a detailed study of various Galois theories, each step getting more abstract than one prior to it. We prove almost all results that we use, except those which would unnecessary lengthen the text.

Contents

Part I
Classical & Modern Galois Theories

1 Classical Galois theory over fields

Let us begin with a quick revision of the concept of the ring of polynomials over a ring R and the most important results therein.

1.1 Review of polynomial rings

Suppose R is a ring, the collection of all polynomials in one variable with coefficients from the ring R has a trivial ring structure (of polynomial addition and multiplication) and is denoted $R[x]$. The $1_{R[x]}$ is the 1_R and $0_{R[x]}$ is 0_R, both treated as constant polynomials. We now have the following basic results:

Proposition 1.1.1. Let F be a field and $F[x]$ be it's polynomial ring. Then each polynomial $f(x) \in F[x]$ of degree n has atmost n zeros, counting multiplicity.

Proof. Given $f(x) \in F[x]$ and the fact that F is a field, an element $a \in F$ is a zero of $f(x)$ if and only if $x-a$ is a factor of $f(x)$ by division algorithm; $\Leftarrow$ is obvious. For $\Rightarrow$, by division algorithm in $F[x]$, which we can do since $F[x]$ is an Euclidean domain as F is a field, therefore for $f(x)$ and $x-a$, we would have unique polynomials $q(x)$ and $r(x)$ with $\deg r(x) = 0$ or $\deg r(x) < \deg(x-a) = 1$, that is, $\deg r(x) = 0$, hence we can write $r(x) = r \in F$ for some constant polynomial. What we have now is $f(x) = (x-a) \cdot q(x) + r$. Now at $x = a$, we have $f(x) = 0 = 0 + r \implies r = 0$, proving the above claim. Therefore $f(x)$ has atmost n zeros. ∎

One can characterize the invertible polynomials (*units*) of the ring $R[x]$ by the following:

Proposition 1.1.2. Let R be a commutative ring with 1. Then a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $R[x]$ is invertible if and only if a_0 is invertible in R and $a_1, \ldots, a_n$ are nilpotent in R.

Proof. ($\Leftarrow$) : If a_0 is invertible and $a_1, \ldots, a_n$ are nilpotent, then we wish to construct an inverse of $f(x)$. Clearly, $a_i x^i$ for $i = 1, \ldots, n$ are nilpotent elements of $R[x]$ as a_i's are. Now because sum of a nilpotent and invertible element is an invertible element, and since $\tilde{f} = a_0^{-1} \cdot a_n x^n + \cdots + a_0^{-1} \cdot a_1 x$ is a nilpotent element and 1 is invertible, therefore $1 + \tilde{f}$ is invertible. Since product of two invertibles is invertible, hence $f = a \cdot (1 + \tilde{f})$ is invertible.
($\Rightarrow$) : Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be invertible. Then there is an another polynomial $g(x) \in R[x]$ with $f(x) \cdot g(x) = 1$. This proves that a_0 must be invertible. To show that all other coefficients are nilpotent, first note that if $f(x) \cdot g(x) = 1$ and $g(x)$ has coefficients b_i, then the coefficient of power m of $f(x) \cdot g(x)$ would be $\sum_{i+j=m} a_i \cdot b_j = 0$. Now unraveling the equations for each m would give us that a_n is nilpotent. Again, because invertible added with nilpotent is invertible, therefore $f(x) - a_n x^n$ is invertible, and so by induction we would get that all $a_1, \ldots, a_n$ are nilpotent. ∎

Corollary 1.1.3. If F is a field, then $f(x) \in F[x]$ is invertible if and only if $f(x)$ is some non-zero constant polynomial.

With this, we now define the important concept of irreducibility of a polynomial:

Definition 1.1.4. (**Irreducible Polynomial**) *Suppose R is a commutative ring with 1 and $R[x]$ be the corresponding polynomial ring. A polynomial $f(x) \in R[x]$ is said to be irreducible if*

$$\forall g(x), h(x) \in R[x] \text{ such that } f(x) = g(x) \cdot h(x) \implies g(x) \text{ or } h(x) \text{ is invertible.}$$

We next state some important classical results without proofs:

Theorem 1. (mod p**-Irreducibility Test**) Let p be a prime and $f(x) \in \mathbb{Z}[x]$. Denote $\bar{f}(x) \in \mathbb{Z}_p[x]$ to be the polynomial obtained by reducing coefficients mod p. If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p[x]$ and $\deg \bar{f}(x) = \deg f(x)$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Theorem 2. (**Eisenstein's Criterion**) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}[x]$. Suppose p is a prime such that

$$p \not| a_n \ \& \ p | a_i \forall i = 0, \ldots, n-1 \ \& \ p^2 \not| a_0,$$

then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

We now begin our inquiry on the classical Galois theory for fields.

1.2 Field extensions

A **field extension** of the field F is just a field $K \supset F$ which contains F and it is denoted as $[K : F]$. Note that a field extension $K \supset F$ can be regarded as an F-vector space where the scalar multiplication is just the multiplication in K with elements of F. The **dimension** of this F-vector space is denoted $\dim[K : F]$. Remember that every field homomorphism is injective and every field has only trivial ideals.

Definition 1.2.1. (**Algebraic Extension**) *Suppose $K \supseteq F$ is a field extension. Then K is said to be an algebraic extension of F if*

$$\forall k \in K \ , \ \exists \text{ non-zero } f(x) \in F[X] \text{ such that } f(k) = 0.$$

Remark 1.2.2. One must note that it is entirely possible that the field extension $[K : F]$ may have a polynomial $f(x) \in K[x]$ which cannot be written entirely in linear factors in $K[x]$, that is, $f(x)$ may not of all roots in K. This is important as those field extensions where indeed each polynomial has all roots in K are called normal extensions, which is studied later.

A field extension $[K : F]$ is algebraic if K treated as F-vector space is finite dimensional:

Proposition 1.2.3. Suppose $[K : F]$ is a field extension. If $[K : F]$ is finite dimensional, then $[K : F]$ is algebraic.

Proof. Take any $a \in K$, we wish to show that $\exists f(x) \in F[x]$ such that $f(a) = 0$. We are given that $[K : F]$ is finite-dimensional, this means that there is an independent set of basis $\{b_1, \cdots, b_n\} \subset K$ such that for any such $a \in K$, if $\sum_{i=1}^{n} c_i b_i = 0$, then $c_i = 0 \forall i$ where $c_i \in F$. Now, note that for each of the term $1, a, a^2, \ldots, a^m$, we have coefficients $c_j^i \in F$ such that $a^i = \sum_{j=1}^{n} c_j^i b_j$ as b_j's are the basis vectors. Now, we wish to find existence of coefficients $k_i \in F$ such that $\sum_{i=0}^{m} k_i a^i = 0 \iff \sum_{i=0}^{m} k_i \left(\sum_{j=1}^{n} c_j^i b_j \right) = 0 \iff \sum_{i=0}^{m} k_i c_j^i = 0 \forall j$ where this last equivalence holds due to independence of b_j's. Hence, we can now find such k_i as in a $[K : F]$ treated as a vector space, any finite collection of elements of K (here c_j^i) have coefficients (here k_i) whose linear combination would indeed be 0. ■

We next study the notion of the minimal polynomial corresponding to an *algebraic element* in a field extension. First we define what is an algebraic element of a field extension:

Definition 1.2.4. (**Algebraic Element of a Field Extension**) *Suppose $[K : F]$ is a field extension. An element $k \in K$ is algebraic over F if:*

$$\exists \text{ non-zero } f(x) \in F[x] \text{ such that } f(k) = 0.$$

Definition 1.2.5. (**Minimal Polynomial of an Algebraic Element**) *Let $[K : F]$ be a field extension and $k \in K$ be an algebraic element over F. Then $f_k(x) \in F[x]$ is called the minimal polynomial of k if $f_k(x)$ is the unique irreducible polynomial with the least degree in the set $\{g(x) \in F[x] \mid g(k) = 0\}$.*

Remark 1.2.6. (***Justification of Definition 1.2.5***) The irreducibility of such $f_k(x)$ is given by the fact that if $f_k(x) = g(x) \cdot h(x)$, then both g and h has degree less that f_k and one of them must have the root as k, contradicting the minimality of f_k to show it is irreducible. To show the uniqueness, let f and g both be minimal for k. Since F is a field, we can safely assume f and g to be monic. Then $f - g$ has k as a root but is of lower degree than possible as the leading term is canceled, hence $f - g$ must be 0.

There is an interesting way to construct the smallest field extension which contains an algebraic element, by constructing the quotient polynomial ring with the principal ideal of minimal polynomial. We first define the following:

Definition 1.2.7. (**Field Generated by an Algebraic Element**) *Suppose $[K : F]$ is a field extension and $k \in K$ is an algebraic element over F. Then, the smallest subfield of K which contains F and k is denoted $F(k)$ and is called the field generated by $k \in K$ for extension $[K : F]$.*

One can easily see that this subfield $F(k)$ is just the set of all evaluation at k of polynomials in $F[x]$:

Lemma 1.2.8. Suppose $[K : F]$ is a field extension and $k \in K$ is algebraic over F. Then, we have

$$F(k) = \{g(k) \mid g(x) \in F[x]\}.$$

Proof. Consider the $F(k)$ as F-subalgebra of K. Then, it is clear that $F(k) = \{g(k) \mid g(x) \in F[x]\}$. We need to show that $F(k)$ is indeed a subfield of K. For this, we need to show that any $a \in F(k)$ is invertible. A general method to show that a given element a of an algebra is invertible or not is to consider the endomorphism of multiplication by a, if it is an isomorphism, which is usually simpler to show, then a is invertible. We use the same technique here, considering $- \cdot a : K \to K$. Since K is a field, this map is injective, and thus, so it's restriction on $F(k)$. Also, $F(k)$ is an F-vector space and the given map is an injective endomorphism, thus by fundamental result of linear operators, this map is also surjective, and thus isomorphic. Hence $- \cdot a : F(k) \to F(k)$ is an isomorphism as a F-algebra map and thus a is invertible. Conversely, take any $g(x) \in F[x]$. Since $g(k)$ would be the linear combination of elements of F and k, therefore $g(k) \in F(k)$. Hence $\{g(k) \mid g(x) \in F[x]\} \subset F(k)$. This yields the proof. ∎

The following gives an alternate realization of the generated field $F(k)$ in terms of a quotient of $F[x]$:

Proposition 1.2.9. Suppose $[K : F]$ is a field extension and $k \in K$ is an algebraic element over F and also let $f_k(x) \in F[x]$ be the minimal polynomial corresponding to k. Then, the smallest subfield $F(k)$ which contains both F and k is isomorphic to the quotient ring $F[x]/\langle f_k(x)\rangle$, i.e

$$F(k) \cong \frac{F[x]}{\langle f_k(x)\rangle}.$$

Proof. Consider the following ring homomorphism:

$$\begin{aligned} \alpha : \frac{F[x]}{(f_K(x))} &\longrightarrow F(k) \\ p(x) + (f_k(x)) &\longmapsto p(k) + (f_k(k)) = p(k), \quad \text{where } \deg p < \deg f_k. \end{aligned}$$

Now because in $F[x]/(f_K(x))$, there is a representative $t(x)$ of $t(x)+(f_k(x))$ whose degree is always less than that of f_k, otherwise we can accommodate the lower terms of $t(x)$ into a multiple of $f_k(x)$ as F is a field, hence α is well-defined. If $p(k) = q(k)$, then $p(k) - q(k) = 0$. But then $p - q$ must have degree more than or equal to that of $f_k(x)$ as f_k is minimal with this property, which cannot happen as $\deg p, \deg q < \deg f_k$. Hence $p - q = 0$ or simply $p = q$. This shows that α is injective. Now take any $a \in F(k)$, then by Lemma 1.2.8, there is a polynomial $p(x) \in F[x]$ with $p(k) = a$. Clearly, $\alpha(p(x) + (f_k(x))) = a$. Hence α is surjective, which establishes the said isomorphism. ∎

It is interesting to note that in our prototypical algebraic field extension $[\mathbb{C} : \mathbb{R}]$, the conjugate complex numbers $a + bi$ and $a - bi$ have the same minimal polynomial $(x - (a + bi))(x - (a - bi)) \in \mathbb{R}[x]$. This can be generalized to an arbitrary field extension as in the following definition:

Definition 1.2.10. (**Conjugate Algebraic Elements of a Field Extension**) *Suppose $[K : F]$ is a field extension and $k_1, k_2 \in K$ are algebraic over F. Then, k_1 and k_2 are defined to be conjugate if the minimal polynomials of both k_1, k_2 are same, that is, if f_{k_1} & f_{k_2} in $F[x]$ are minimal polynomials of k_1 & k_2 respectively, then*

$$f_{k_1}(x) = f_{k_2}(x).$$

In topology, a retract of a continuous endomorphism to a subspace is such a map which fixes the subspace (is 1 for the subspace). We have a similar definition for a given field extension:

Definition 1.2.11. (F-**Homomorphism**) *Let $[K : F]$ be a field extension. A field homomorphism $f : K \rightarrowtail K$ is called an F-homomorphism if the restriction $f|_F$ is identity 1_F. More diagrammatically, if the following commutes:*

$$\begin{array}{ccc} K & & \\ {\scriptstyle\iota}\uparrow & \searrow^{f} & \\ F & \xhookrightarrow[\iota]{} & K \end{array} .$$

We now see that any F-homomorphism is an automorphism if the extension is algebraic:

Proposition 1.2.12. Suppose $[K : F]$ is an algebraic field extension. Let $f : K \rightarrowtail K$ be an F-homomorphism. Then, f is an automorphism.

Proof. We only need to show that an F-homomorphism is a surjection as all field homomorphisms are already injections. To this end, take any $k \in K \backslash F$. Since $[K : F]$ is algebraic so we have a unique irreducible least degree polynomial $p(x) \in F[x]$ such that $p(k) = 0$. But because of f being an F-homomorphism, we have that for any $a \in F$, $f(a \cdot k) = f(a) \cdot f(k) = a \cdot f(k)$, which means that $f(p(x)) = p(f(x))$, which further means that $f(k)$ is also a root of $p(x)$. We wish to show that $p(x)$ is also minimal for $f(k)$. Suppose that is not the case, that is $p(x)$ is not minimal for $f(k)$, but then it's minimal polynomial $q(x)$ would have to be minimal for k too, but $p(x)$ is minimal for k, therefore $p(x) = q(x)$. Hence $p(x)$ is minimal for both k and $f(k)$, that is, k and $f(k)$ are conjugate. Now consider the set of zeroes of $p(x)$ in K, $Z(p(x)) := \{t \in K \mid p(t) = 0\}$. The function f cycles through the elements of $Z(p(x))$ because of the fact $f(p(x)) = p(f(x))$. Hence we have the function $f|_{Z(p(x))} : Z(p(x)) \longrightarrow Z(p(x))$. We need to show that this is a bijection. Injection is trivial because f is injective. To show surjection, take any root $r \in Z(p(x))$. We just need to show that $f^n(r) = r$ for some $n \in \mathbb{N}$. Because $Z(p(x))$ is finite, therefore this is impossible only if there is a root $r' \in Z(p(x))$ such that $\exists m \in \mathbb{N}$ such that $f^{i+m}(r') = f^i(r')\ \forall i = 0, 1, \ldots$. But this is possible only if $r' \in F$, which is not possible because if $p(x)$ has a root in F, then $\exists n \in \mathbb{N}$ such that $f^n(k) = r = f(r) = f(f(r)) = \cdots = f^n(r)$, then by injectivity of f, we have that $k = r$ but $k \in K \setminus F$ and $r \in F$, hence a contradiction. So $f|_{Z(p(x))}$ is a bijection. Therefore, $\exists l \in \mathbb{N}$ such that $f^l(k) = f(f^{l-1}(k)) = k$, hence f is surjective. Hence proved. ■

Remark 1.2.13. Proposition 1.2.12 hence shows the importance of F-homomorphisms for a field extension $[F : K]$. We therefore denote $\mathbf{Aut}_F(K)$ as the group of all F-homomorphisms (which are also automorphisms as just proved) of a field extension $[F : K]$ with the composition operation.

1.3 Separable extensions

We now study the separability of a field extension. The notion of *separability* here is quite particular. First we must remind ourselves of the definition of derivative of a polynomial:

Definition 1.3.1. (**Derivative of a Polynomial**) *Suppose F is a field and $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial in $F[x]$. The derivative of $p(x)$ is again a polynomial $p'(x) \in F[x]$ given as follows:*

$$p'(x) := na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

Remark 1.3.2. Few remarks are in order for the Definition 1.3.1:

1. $\deg p'(x) = n - 1$ if and only if characteristic of F doesn't divide n.
2. It must be noted that it is **not** true in general for a polynomial $p(x) \in F[x]$ where F is a field, that $\deg p'(x) < \deg p(x)$. A counter example can be when field F has characteristic 2 and the polynomial $p(x) = x^2 - 1$. Clearly, $p'(x) = 2 \cdot x = 0$, which means that $\deg p'$ is undefined but $\deg p(x) = 2$. Hence to talk about the decrease in degree of derivatives, we strictly use the 1 above.
3. If the characteristic of the field F divides n, then $n \cdot a_n = 0$, thus making the degree of $p'(x)$ $n - 2$.
4. For $p(x), q(x) \in F[x]$, $(p(x) + q(x))' = p'(x) + q'(x)$ and $(p(x) \cdot q(x))' = p'(x) \cdot q(x) + p(x) \cdot q'(x)$.

The derivative of a polynomial can be used to derive information about the multiplicity of a given root:

Proposition 1.3.3. Suppose F is a field and $p(x) \in F[x]$ is a polynomial. Then, a root $r \in F$ of $p(x)$ is a multiple[3] root of $p(x)$ if and only if $p(r) = 0$ and $p'(r) = 0$.[4]

Proof. (L $\implies$ R) Suppose $r \in F$ is a multiple root of $p(x)$. Then we can write $p(x) = (x-r)^m \cdot q(x)$ where m is the multiplicity of the root r and $q(x) \in F[x]$. Then, $p'(x) = m(x-r)^{m-1} \cdot q(x) + q'(x) \cdot (x-r)^m$. Evaluating $p'(x)$ at $x = r$, we have $p'(r) = 0$.
(R $\implies$ L) Suppose $r \in F$ is a root of $p(x)$ such that $p'(r) = 0$. Now, $p(x)$ can be written as $p(x) = (x-r) \cdot q(x)$. Since $p'(x) = q(x) + (x-r) \cdot q'(x)$ and we know that $p'(r) = 0$, therefore $p'(r) = q(r) = 0$. That is, $q(x) = (x-r) \cdot u(x)$ for some other $u(x) \in F[x]$. Hence, $p(x) = (x-r) \cdot (x-r) \cdot u(x) = (x-r)^2 \cdot u(x)$. Hence r is a multiple root of $p(x)$. ■

The definition of separability can now be stated:

Definition 1.3.4. (**Separable Field Extension**) *Suppose $[K : F]$ is a field extension. This extension is defined to be separable if*

1. *$[K : F]$ is algebraic,*
2. *For each $k \in K$, the minimal polynomial $f_k(x) \in F[x]$ has all simple roots (no multiple roots).*

Remark 1.3.5. By the help of Proposition 1.3.3, one can check whether an algebraic field extension $[K : F]$ is separable by checking for each $k \in K$ whether the derivative of minimal polynomial $f_k'(x)$ is zero or not for each root r of f_k. If for each root r, f_k' is not zero then f_k has no multiple roots and hence $[K : F]$ is separable.

Another result which would help us determining a separable extension is the following:

Proposition 1.3.6. Suppose $[K : F]$ is a field extension. Additionally suppose that K (and so, F) is a field of characteristic 0. If $k \in K$ is algebraic over F, then all roots of the minimal polynomial $f_k(x)$ are simple.

[3] A root r of a polynomial $p(x)$ is multiple if $p(x) = (x-r)^m \cdot q(x)$ where m is finite. A root which appears only once as a linear factor of $p(x)$ is termed a ***simple*** root.

[4] This helps in showing that in a field of characteristic p, there is only one root with multiplicity p of the polynomial $x^p - \alpha$ for any $\alpha \in K$. In particular, it says that the group of roots of unity is trivial in the case of characteristic p, which is quite sad (but maybe Picard will make us happy again!?).

Proof. Take $k \in K$ which is algebraic and denote $f_k(x) \in F[x]$ as the minimal polynomial of k. We only need to check for simplicity of the root k of $f_k(x)$ as any other root of $f_k(x)$ cannot be multiple otherwise we can have a polynomial of degree less than that of $f_k(x)$ which also has k as it's root. Now suppose k is a multiple root of $f_k(x)$, which is equivalent to saying, by Proposition 1.3.3, that $f_k'(k) = 0$. But $\deg f_k'(x) = \deg f_k(x) - 1 < \deg f_k(x)$ because characteristic of F doesn't divide $\deg f_k(x)$ (in-fact it doesn't divide any element of F as it is 0), which contradicts the minimality of f_k. Hence k is simple root of $f_k(x)$, and so all the roots of $f_k(x)$ are simple. ■

We then have that a characteristic zero algebraic field extension is separable also:

Corollary 1.3.7. Suppose F is a field of characteristic 0 and $[K : F]$ is a field extension. If $[K : F]$ is algebraic, then $[K : F]$ is separable.

Proof. Trivially follows from Proposition 1.3.6 as all elements of K are algebraic now. ■

Finally, we take a glimpse at intermediate field extensions and note the following result on how separability transverses between such extensions:

Proposition 1.3.8. Suppose $[K : F : P]$ be field extensions ($K \supseteq F \supseteq P$). If $[K : P]$ is separable, then $[K : F]$ is separable.

Proof. The extension $[K : F]$ is algebraic because for each $k \in K$, $\exists\ f(x) \in P[x] \subseteq F[x]$ such that $f(k) = 0$. Now, take any $k \in K$ and consider the minimal polynomial $f_k(x) \in P[x]$ which has all simple roots as $[K : P]$ is separable. Now denote $g_k(x) \in F[x]$ as the minimal polynomial of $k \in K$ for the algebraic extension $[K : F]$. We have to show that $g_k(x)$ has all simple roots. Since $F[x] \supseteq P[x]$, therefore let us consider $f_k(x) \in P[x]$ as a member of $F[x]$. Also, $\deg f_k \geq \deg g_k$ because if we assume $\deg f_k < \deg g_k$, then the minimality of $g_k(x)$ is challenged by $f_k(x)$. Now, by division algorithm in $F[x]$, we have $f_k(x) = g_k(x) \cdot q(x) + r(x)$ for unique polynomials $q(x), r(x) \in F[x]$ with $\deg r(x) < \deg g_k(x)$. Now, if we evaluate the above equation at $x = k$, we get, $f_k(k) = g_k(k) \cdot q(k) + r(k) \implies r(k) = 0$. But $\deg r(x) < \deg g_k(x)$, therefore to make sure $g_k(x)$ remains minimal for $[K : F]$, $r(x)$ must be 0. But then $f_k(x) = g_k(x) \cdot q(x)$ and therefore all roots of $g_k(x)$ are roots of $f_k(x)$. But $f_k(x)$ has all simple roots therefore $g_k(x)$ has all simple roots. ■

1.4 Normal extensions

We now study field extensions where all roots of the minimal polynomial lies only in the extension:

Definition 1.4.1. (**Normal Field Extension**) *Suppose $[K : F]$ is a field extension. This extension is defined to be normal if*

1. *$[K : F]$ is algebraic,*
2. *For each $k \in K$, the minimal polynomial $f_k(x) \in F[x]$ factors entirely in $K[x]$ in polynomials of degree 1, or equivalently, $f_k(x) \in F[x]$ has all roots in K.*

Remark 1.4.2. If $[K : F]$ is an algebraic extension and K is an algebraically closed field[5], then $[K : F]$ is trivially normal.

The normality of an extension traverses:

Proposition 1.4.3. Suppose $[K : F : P]$ are field extensions ($K \supseteq F \supseteq P$). If $[K : P]$ is normal, then $[F : P]$ is normal.

[5]A field K is algebraically closed if each polynomial in $K[x]$ has atleast one root in K, which is equivalent to stating that if each polynomial in $K[x]$ has all roots in K.

Proof. Exactly that of Proposition 1.3.8. ■

The next result establishes our first relation between an F-homomorphism and intermediate field extensions:

Proposition 1.4.4. Suppose $[K : P]$ is a normal field extension which is additionally finite dimensional as a P-vector space. If $[K : F : P]$ is any intermediate field extension, then every P-homomorphism $F \rightarrowtail K$ extends to a P-automorphism of K.

Proof. Take an element $k \in K$ and a P-homomorphism $f : F \rightarrowtail K$. We first wish to show that this P-homomorphism extends to a P-homomorphism $\bar{f} : F(k) \rightarrowtail K$. In-fact, because $[K : P]$ is finite-dimensional, hence if we could show that f extends as before, then repeating the same process (by setting $F(k) = (F(k))(k')$ for any other $k' \in K$ and so on) finite times would give us a P-homomorphism $K \rightarrowtail K$, which by Proposition 1.2.12 would be a P-automorphism, hence proving the result. Therefore our sole aim now is to extend $f : F \rightarrowtail K$ to $\bar{f} : F(k) \rightarrowtail K$.
In order to do this, we first note that $[K : F]$ is finite-dimensional because $[K : P]$ is, and so by Proposition 1.2.3, the extension $[K : F]$ is algebraic. Now let $p_k(x) \in P[x]$ be the k's minimal polynomial in $[K : P]$ and let $q_k(x) \in F[x]$ be the k's minimal polynomial in $[K : F]$. Since $P[x] \subseteq F[x]$, therefore $p_k(x) \in F[x]$. But $q_k(x) \in F[x]$ is minimal for k, therefore $q_k(x)$ divides $p_k(x)$ in $F[x]$. But $[K : P]$ is normal, therefore $p_k(x)$ is completely linearly factored in K and therefore so does $q_k(x)$. That is, $q_k(x)$ also has all roots in K.
Now, we have a canonical ring homomorphism:

$$\begin{aligned} \hat{f} : F[x] &\longrightarrow K[x] \\ \sum_{i=0}^{n} a_n x^n &\longmapsto \sum_{i=0}^{n} f(a_n) x^n. \end{aligned}$$

Clearly, $\hat{f}\Big|_{P[x]} = 1_{P[x]}$. Due to this, $\hat{f}(p_k(x)) = p_k(x) \in K[x]$ and $\hat{f}(q_k(x)) \in K[x]$. Since $q_k(x)$ divides $p_k(x)$ in $F[x]$ and $\hat{f}$ is ring homomorphism, therefore $\hat{f}(q_k(x))$ divides $\hat{f}(p_k(x)) = p_k(x)$ in $K[x]$. Again, as $p_k(x)$ has all roots in $K[x]$, therefore $\hat{f}(q_k(x))$ also is completely linearly factored in $K[x]$. Now for any root of $\hat{f}(q_k(x))$, say $r \in K$, which would be a root of $p_k(x)$ too, we first have that $(x-r) \in K[x]$ is the minimal polynomial of r and $\hat{f}(q_k(x)) \in \langle (x-r) \rangle$. Since $\hat{f} : F[x] \longrightarrow K[x]$ is a ring homomorphism, therefore we have a ring homomorphism between quotients $\bar{f} : \dfrac{F[x]}{\langle q_k(x) \rangle} \longrightarrow \dfrac{K[x]}{\langle (x-r) \rangle}$, which takes the representative to it's image by $\hat{f}$. But because of Proposition 1.2.9, we have the following P-homomorphism:

$$\begin{aligned} \bar{f} : F(k) \cong \frac{F[x]}{\langle q_k(x) \rangle} &\longrightarrow \frac{K[x]}{\langle (x-r) \rangle} \cong K(r) \cong K \\ g(x) + \langle q_k(x) \rangle &\longmapsto \hat{f}(g(x)) + \langle (x-r) \rangle . \end{aligned}$$

Hence, we have extended a P-homomorphism $f : F \rightarrowtail K$ to a P-homomorphism $\bar{f} : F(k) \rightarrowtail K$, proving the result. ■

In a finite-dimensional normal field extension, there is an equivalent condition to check whether two elements are conjugate:

Proposition 1.4.5. Suppose $[K : F]$ is a finite-dimensional normal field extension. Then, two elements $k_1, k_2 \in K$ are conjugate if and only if $\exists$ an F-automorphism $f : K \rightarrowtail K$ such that $f(k_1) = k_2$.

Proof. (L $\implies$ R) Suppose $k_1, k_2 \in K$ are conjugate and hence let $p(x) \in F[x]$ be their common minimal polynomial. Consider the field $F(k_1)$. By Proposition 1.2.9, $F(k_1) \cong \dfrac{K[x]}{\langle p(x) \rangle} \cong F(k_2)$, and denote this as

the F-isomorphism $\bar{f} : F(k_1) \rightarrowtail F(k_2)$, which can be written as a F-homomorphism $\bar{f} : F(k_1) \rightarrowtail K$ such that $\bar{f}(k_1) = k_2$. Note we now have the intermediate extension $[K : F(k_1) : F]$, hence by Proposition 1.4.4, $\bar{f} : F(k_1) \rightarrowtail K$ can be extended to a F-automorphism $f : K \rightarrowtail K$ with $f(k_1) = k_2$.
(R $\implies$ L) Suppose we have an F-automorphism $f : K \rightarrowtail K$ with $f(k_1) = k_2$ for some $k_1, k_2 \in K$. Let $p(x) \in F[x]$ be the minimal polynomial of k_1 and let $q(x) \in F[x]$ be the minimal for k_2. Therefore $p(k_1) = 0 \implies f(p(k_1)) = f(0) \implies p(f(k_1)) = 0 \implies p(k_2) = 0$. But then $\exists s(x) \in F[x]$ such that $p(x) = q(x) \cdot s(x)$ because $q(x)$ is minimal for k_2. Now, $p(k_1) = q(k_1) \cdot s(k_1) \implies 0 = q(k_1) \cdot s(k_1)$. Since $F[x]$ is an integral domain as F is a field, therefore either $s(k_1) = 0$ or $q(k_1) = 0$. But since $\deg q(x) \leq \deg p(x)$ and $\deg q(x) \neq 0$, therefore if $q(k_1) = 0$, then $q(x) = p(x)$ as $p(x)$ is minimal for k_1. If $s(k_1) = 0$, then because $\deg s(x) < \deg p(x)$, we must have that $s(x) = 0$ as $p(x)$ is minimal for k_1, but then $p(x) = 0$ which is a contradiction. Hence we only have $q(x) = p(x)$, that is, k_1 and k_2 have same minimal polynomials. ■

We will now finally study the Galois Extensions and the main theorem of classical Galois theory.

1.5 Galois extensions

A Galois extension is defined as an amalgamation of past sections:

Definition 1.5.1. (**Galois Field Extension**) *Suppose $[K : F]$ is a field extension. This extension $[K : F]$ is defined to be Galois if $[K : F]$ is both normal and separable field extension.*

An easy lemma is the following:

Proposition 1.5.2. Suppose $[K : F : P]$ are field extensions ($K \supseteq F \supseteq P$). If $[K : P]$ is Galois, then $[K : F]$ is Galois.

Proof. Since $[K : P]$ is normal and separable, then $[K : F]$ is normal and separable by Proposition 1.3.8 and 1.4.3. ■

To each field extension $[K : F]$, we have the group of F-automorphisms of K. When $[K : F]$ is Galois, we call this group the Galois group:

Definition 1.5.3. (**Galois Group of a Galois Extension**) *Suppose $[K : F]$ is a Galois field extension. Then the group of all F-automorphisms of K, $\mathbf{Aut}_F(K)$, is called the Galois group of the extension $[K : F]$ and is denoted:*

$$\mathbf{Gal}\,[K : F].$$

Remark 1.5.4. For each subgroup $G \leq \mathbf{Gal}\,[K : F]$, there is a corresponding intermediate field extension of $[K : F]$ given by:

$$\mathbf{Fix}\,(G) := \{k \in K \mid g(k) = k \; \forall g \in G\}.$$

Clearly, $F \subseteq \mathbf{Fix}\,(G) \subseteq K$ and $\mathbf{Fix}\,(G)$ is a subfield with same operation from that of F. Hence, we have the intermediate extension $[K : \mathbf{Fix}\,(G) : F]$ for each subgroup $G \leq \mathbf{Gal}\,[K : F]$.

The following is the usual example of an Adjoint Functor between two posets treated as categories:

Definition 1.5.5. (**Galois Connection**) *Suppose $(A, \leq_A)$ and $(B, \leq_B)$ are two partially ordered sets. A Galois connection between A and B is given by a pair of two order reversing functions,*

$$A \underset{g}{\overset{f}{\rightleftarrows}} B$$

which means that if $a_1 \leq_A a_2$ *in* A*, then* $f(a_2) \leq_B f(a_1)$ *in* B *and similarly if* $b_1 \leq_B b_2$ *in* B*, then* $g(b_2) \leq_B g(b_1)$ *in* A*, with the property that*

$$a \leq g \circ f(a) \;\; \& \;\; b \leq f \circ g(b)$$

for all $a \in A$ *and* $b \in B$*.*

We have the following Galois connection:

Proposition 1.5.6. Let $[K : P]$ be a Galois field extension. The maps:

$$\{F \mid K \supseteq F \supseteq P\} \underset{\textbf{Fix}(-)}{\overset{\textbf{Gal}\,(-)}{\rightleftarrows}} \{G \mid G \leq \textbf{Gal}\,[K : F] \; \forall \; F \text{ with } K \supseteq F \supseteq P\}$$

where $\textbf{Gal}\; F := \textbf{Gal}\;[K : F]$ forms a Galois connection.

Proof. Clearly, $\{F \mid K \supseteq F \supseteq P\}$ and $\{G \mid G \leq \textbf{Gal}\,[K : F]\}$ are both posets under inclusion. Next, we wish to show that $\textbf{Gal}\,(-)$ and $\textbf{Fix}\,(-)$ are order reversing maps[6]. Take $F_1 \subseteq F_2$ and take $g \in \textbf{Gal}\,[K : F_2]$. Since $g : K \rightarrowtail K$ is an F_2-automorphism, so g is an F_1-automorphism also, and so $g \in \textbf{Gal}\,[K : F_1]$. Similarly, for two subgroups $G_1 \subseteq G_2$ of $\textbf{Gal}\,[K : F]$, for any $a \in \textbf{Fix}\,(G_2)$ is such that $g(a) = a \forall g \in G_2$. But $G_1 \subseteq G_2$, therefore $g(a) = a \forall g \in G_1$, and so $g \in \textbf{Fix}\,(G_1)$ which shows that $\textbf{Fix}\,(G_2) \subseteq \textbf{Fix}\,(G_1)$. Hence $\textbf{Gal}\,(-)$ and $\textbf{Fix}\,(-)$ are both contravariant functors. We now wish to show that for any intermediate extension $[K : F : P]$ of $[K : P]$, we have $F \subseteq \textbf{Fix}\,(\textbf{Gal}\,[K : F])$. Take any $a \in F$. Since $g(a) = a \forall g \in \textbf{Gal}\,[K : F]$ because g is an F-automorphism by definition, therefore $a \in \textbf{Fix}\,(\textbf{Gal}\,[K : F])$. Hence shown. Similarly, we wish to show that for any subgroup G of any Galois group $\textbf{Gal}\,[K : F]$ of any intermediate extension F, we have $G \leq \textbf{Gal}\,[K : \textbf{Fix}\,(G)]$. For this, take any $g \in G$. This g is an F-automorphism of K. Since $g(x) = x \; \forall x \in \textbf{Fix}\,(G)$ because $\textbf{Fix}\,(G) = \{k \in K \mid r(k) = k \; \forall r \in G\}$, therefore g is also a $\textbf{Fix}\,(G)$-automorphism of K, and hence $g \in \textbf{Gal}\,[K : \textbf{Fix}\,(G)]$. Hence proved. ■

Remark 1.5.7. It must be noted that $\textbf{Gal}\,(-) : \{F \mid K \supseteq F \supseteq P\}^{op} \longrightarrow \{G \mid G \leq \textbf{Gal}\,[K : F] \; \forall \; F \text{ with } K \supseteq F \supseteq P\}$ is a contravariant functor and so is $\textbf{Fix}\,(-) : \{G \mid G \leq \textbf{Gal}\,[K : F] \; \forall \; F \text{ with } K \supseteq F \supseteq P\}^{op} \longrightarrow \{F \mid K \supseteq F \supseteq P\}$.

1.5.1 The fundamental theorem of classical Galois theory

We finally state and prove the main theorem of Galois theory, which shows that the above adjunction is actually an isomorphism when extension is finite-dimensional:

Theorem 3. (**Fundamental Theorem of Classical Galois Theory**) Suppose $[K : P]$ is a finite-dimensional Galois field extension. Then, for each intermediate extension $K \supseteq F \supseteq P$, we have that

$$\dim[K : F] = |\textbf{Gal}\,[K : F]|\,.$$

Moreover, it then follows that the following Galois connection

$$\{F \mid K \supseteq F \supseteq P\} \underset{\textbf{Fix}(-)}{\overset{\textbf{Gal}\,[K:-]}{\rightleftarrows}} \{G \mid G \leq \textbf{Gal}\,[K : F] \; \forall \; F \text{ with } K \supseteq F \supseteq P\}$$

is an isomorphism of posets[7].

[6]Equivalently, they are contravariant functors between the respective posets treated as categories.

[7]One must note that $\textbf{Gal}\,[K : F] \leq \textbf{Gal}\,[K : P]$, therefore we simply have $\{G \mid G \leq \textbf{Gal}\,[K : F] \; \forall \; F \text{ with } K \supseteq F \supseteq P\} = \{G \mid G \leq \textbf{Gal}\,[K : P]\}$.

Proof. We prove the result in the following 2 acts.
Act 1. *Proving* $\dim[K:F] = \textbf{Gal}\,[K:F]$ *by Strong Induction.*
We will apply strong induction on the $\dim[K:F]$ for any arbitrary intermediate extension F as in $[K:F:P]$.
Scene 1.1. *Base Case of Strong Induction.*
The base case can be scene quite easily because if $\dim[K:F]=1$, then $\exists b \in K$ such that for any $k \in K$, $\exists c \in F$ such that $k = c\cdot b$. For $k=1$, we have $1 = c\cdot b \implies c^{-1} = b$. But $c \in F$ and so $c^{-1} \in F$, hence $c^{-1} = b \in F$. Therefore each element $k \in K$ is in F, hence $K = F$. Then there is only one trivial F-automorphism of K, the identity. Hence $|\textbf{Gal}\,[K:F]| = 1 = \dim[K:F]$.
Scene 1.2. *General Case of Strong Induction.*
Now suppose $\dim[K:F] = n$. We now, as per the rules of strong induction, assume that for any intermediate extension $[K:F:P]$ with $\dim[K:F] < n$ we have

$$\dim[K:F] = |\textbf{Gal}\,[K:F]|\,.$$

Take any $k \in K$ and denote by $p_k(x) \in F[x]$ the minimal polynomial of k. Now, we observe the following facts:

- **Fact 1.2.1.** $\dim[K:F(k)] < n$.
- **Fact 1.2.2.** $\dim[K:F(k)] = \deg p_k(x)$.
- **Fact 1.2.3.** $\dim[F(k):F]\times\dim[K:F(k)] = \dim[K:F]$.

Let us now denote $r = \deg p_k(x)$. With the above three facts, we have the following result:

$$\dim[K:F(k)] = \frac{n}{r} < n.$$

But the inductive argument guarantees that $\dim[K:F] = |\textbf{Gal}\,[K:F]|$ whenever $\dim[K:F] < n$, which is the case with $\dim[K:F(k)] = n/r$. Therefore we have n/r $F(k)$-automorphisms denoted $f_1,\ldots,f_{\frac{n}{r}} : K \rightarrowtail K$. We also have the fact $p_k(x)$ has r roots in K ($[K:F]$ is normal and finite-dimensional). Let $k_1,\ldots,k_r$ be those roots of $p_k(x)$. By Proposition 1.4.5, we have that there are r F-automorphisms of K denoted by $g_1\ldots,g_r : K \rightarrowtail K$ such that $g_i(k) = k_i$. We then have the following n F-automorphisms:

$$h_{ij} = g_j \circ f_i \;\forall\; i = 1,\ldots,\frac{n}{r},\; j = 1,\ldots,r.$$

Our claim is that these n automorphisms precisely are the n members of $\textbf{Gal}\,[K:F]$. To see this, we first have to be sure that all h_{ij}'s are distinct. To this extent, let us assume that $h_{ij} = h_{i'j'}$. This means that $h_{ij}(k) = h_{i'j'}(k) \implies g_j\circ f_i(k) = g_{j'}\circ f_{i'}(k) \implies g_j(k) = g_{j'}(k)$ as $f_i, f_{i'}$ are $F(k)$-automorphisms. This further means that $k_j = k_{j'}$. But since $[K:F]$ is separable, hence each of the root k_i's are distinct and so $k_j = k_{j'} \implies j = j' \implies g_j = g_{j'}$. But since g_j's are monics, therefore $g_j\circ f_i = g_j\circ f_{i'} \implies f_i = f_{i'}$. Hence no two h_{ij}'s are same.
Next thing we wish to show is that each F-automorphism of K from $\textbf{Gal}\,[K:F]$ is actually equal to some h_{ij}. This would indeed complete the proof of the fact that h_{ij}'s are all there is to the group $\textbf{Gal}\,[K:F]$. To this extent, let us take any F-automorphism $f : K \rightarrowtail K$. Note that $p_k(k) = 0 \implies f(p_k(k)) = f(0) = 0 \implies p_k(f(k)) = 0$, therefore $f(k) = k_j$ for some $j = 1,\ldots,r$. Now, note that $g_j^{-1}\circ f$ is such an F-automorphism of K such that $g_j^{-1}\circ f(k) = g_j^{-1}(f(k)) = g_j^{-1}(k_j) = k$. That is, $g_j^{-1}\circ f$ is an $F(k)$-automorphism of K. Hence $g_j^{-1}\circ f = f_i$ for some $i = 1,\ldots,n/r$. This means that $f = g_j\circ f_i = h_{ij}$, hence proved that any F-automorphism of K is indeed equal to some h_{ij}. So, we have proved by the assumption of general case of induction, that if $\dim[K:F] = n$, then $n = \textbf{Gal}\,[K:F]$, completing the proof of Scene 1.2, and so of Act 1.

Act 2. $\mathbf{Fix}\,(-) \vdash \mathbf{Gal}\,(-)$ *is an Isomorphism Pair.*
To show that the above mentioned pair forms an isomorphism, we will show that the counit and unit are identity; for any intermediate extension $K \supseteq F \supseteq P$ and for any subgroup $G \leq \mathbf{Gal}\,[K : F]$, we wish to show that

$$\mathbf{Gal}\,[K : \mathbf{Fix}\,(G)] = G$$

and

$$\mathbf{Fix}\,(\mathbf{Gal}\,[K : F]) = F.$$

Scene 2.1. *Proving that* $G \leq \mathbf{Gal}\,[K : \mathbf{Fix}\,(G)]$.
To show this, we first note that we already have proved by Act 1 that

$$|\mathbf{Gal}\,[K : \mathbf{Fix}\,(G)]| = \dim[K : \mathbf{Fix}\,(G)].$$

This means that we just need to show the following:

$$|G| = \dim[K : \mathbf{Fix}\,(G)].$$

This is simple because $\mathbf{Fix}\,(-) \vdash \mathbf{Gal}\,(-)$ is a Galois connection and therefore we have $G \leq \mathbf{Gal}\,[K : \mathbf{Fix}\,(G)]$, which means that $|G| \leq |\mathbf{Gal}\,[K : \mathbf{Fix}\,(G)]| = \dim[K : \mathbf{Fix}\,(G)]$.
Scene 2.2. *Proving that* $\mathbf{Gal}\,[K : \mathbf{Fix}\,(G)] \leq G$.
This is the most important part of the whole proof of this theorem and the remaining parts will be quite easy. First note that $|G| \leq \mathbf{Gal}\,[K : F] \implies |G| \leq |\mathbf{Gal}\,[K : F]| = \dim[K : F]$. Since $\dim[K : F]$ is finite, therefore $|G| = n$ is finite. We now equivalently wish to prove that $\dim[K : \mathbf{Fix}\,(G)] \leq n$.
To do this let us assume that $\dim[K : \mathbf{Fix}\,(G)] = n + 1$. Let the basis elements of the $\mathbf{Fix}\,(G)$-vector space $[K : \mathbf{Fix}\,(G)]$ be denoted by $k_1, \ldots, k_n, k_{n+1} \in K$. Now denote the n elements of G as $g_1, \ldots, g_n \in G \leq \mathbf{Gal}\,[K : F]$. But because $\mathbf{Fix}\,(G) = \{k \in K \mid g_i(k) = k\ \forall i = 1, \ldots, n\}$, so we consider the following system of equations in the vector space $[K : \mathbf{Fix}\,(G)]$:

$$\begin{aligned} \sum_{i=1}^{n+1} g_1(k_i)x_i &= 0 \\ \vdots &= \vdots \\ \sum_{i=1}^{n+1} g_n(k_i)x_i &= 0. \end{aligned} \tag{1}$$

Since we have n equations and $n+1$ variables, therefore exists atleast one non-zero solution to (1). From the set of all such solutions to the (1), let us select the one for which the amount of non-zero components is minimal. Since the order of the equations in (1) is irrelevant as it amounts to relabeling of g_i's, therefore we can write this minimal polynomial as the following $n+1$ long tuple:

$$(\alpha_0, \alpha_1, \ldots, \alpha_r, 0, 0, \ldots, 0)$$

where $\alpha_i \neq 0 \in K\ \forall i = 0, 1, \ldots, r < n + 1$. It is exactly this non-zero α_i's which would become main culprit behind our sought after contradiction. This minimal solution is clearly the root of the following restricted system of (1):

$$\begin{aligned} \sum_{i=1}^{r} g_1(k_i)x_i &= 0 \\ \vdots &= \vdots \\ \sum_{i=1}^{r} g_n(k_i)x_i &= 0 \end{aligned} \tag{2}$$

where this equation has n equations and $r-1 < n$ variables, which means that (2) admits a solution which is non-zero. One such zero obviously has to be $(\alpha_1, \ldots, \alpha_r)$. Now take any $g \in G$. We then have the following equations:

$$\begin{aligned} \sum_{i=1}^{r} g \cdot g_1(k_i) g(\alpha_i) &= 0 \\ \vdots &= \vdots \\ \sum_{i=1}^{r} g \cdot g_n(k_i) g(\alpha_i) &= 0. \end{aligned} \tag{3}$$

But since G is a subgroup, therefore $g \cdot g_i = g_j$ for some j. Hence the equations in (3) can be just written as follows as g merely permutates the $g_i(k_l)$:

$$\begin{aligned} \sum_{i=1}^{r} g_1(k_i) g(\alpha_i) &= 0 \\ \vdots &= \vdots \\ \sum_{i=1}^{r} g_n(k_i) g(\alpha_i) &= 0. \end{aligned} \tag{4}$$

Now, we form a new system of equations by the manipulation $\alpha_r \times (4) - g(\alpha_r) \times (2)(\alpha_i)$, which gives the following:

$$\begin{aligned} \sum_{i=1}^{r} \left(\alpha_r g(\alpha_i) - g(\alpha_r)\alpha_i\right) g_1(k_i) &= 0 \\ \vdots &= \vdots \\ \sum_{i=1}^{r} \left(\alpha_r g(\alpha_i) - g(\alpha_r)\alpha_i\right) g_n(k_i) &= 0 \end{aligned} \tag{5}$$

This means that we have a solution to system in (2) given by:

$$S = (\alpha_r g(\alpha_1) - g(\alpha_r)\alpha_1, \ldots, \alpha_r g(\alpha_{r-1}) - g(\alpha_{r-1})\alpha_1, 0)$$

which, by appending $n+1-r$ zeros in front of S would give us a solution of (1). But this solution would have $r-1$ zeros, which is not possible as the $(\alpha_0, \ldots, \alpha_r)$ were the minimal non-zero solution by choice. Therefore each entry in S must be zero. This condition gives rise to:

$$\alpha_r g(\alpha_i) - g(\alpha_r)\alpha_i \; \forall i = 1, \ldots, r-1.$$

This can be restated as $g(\alpha_i \cdot \alpha_r^{-1}) = \alpha_i \cdot \alpha_r^{-1} \; \forall i = 1, 2, \ldots, r$. But $g \in G$ was arbitrarily chosen, therefore $g(\alpha_i \cdot \alpha_r^{-1}) = \alpha_i \cdot \alpha_r^{-1} \; \forall g \in G \; \forall i = 1, \ldots, r$. This means that $\alpha_i \cdot \alpha_r^{-1} \in \mathbf{Fix}(G)$. Now write $\alpha_i \cdot \alpha_r^{-1} = m_i \in \mathbf{Fix}(G) \implies \alpha_i = m_i \cdot \alpha_r \; \forall i = 1, \ldots, r-1$. Now because $(\alpha_1, \ldots, \alpha_r)$ is a solution of system (2), it can be seen that

$$\begin{aligned} g_1\left(\sum_{i-1}^{r} k_i m_i\right) &= 0 \\ \vdots &= \vdots \\ g_n\left(\sum_{i-1}^{r} k_i m_i\right) &= 0 \end{aligned}$$

which gives us that $k_1m_1+\cdots+k_rm_r = 0$. But since $k_1, \ldots, k_r$ are members of the basis, so $m_i = \alpha_i \cdot \alpha_r^{-1} = 0$, which is not true, therefore a contradiction. Hence our assumption that $\{k_1, \ldots, k_n, k_{n+1}\}$ is linearly independent is wrong and therefore $\dim[K : \mathbf{Fix}\,(G)] \leq n$.
By combining Scenes 2.1 and 2.2, we have showed that $\mathbf{Gal}\,(-) \circ \mathbf{Fix}\,(-) = 1$.

We now wish to show that $\mathbf{Fix}\,(\mathbf{Gal}\,[K : F]) = F$. We employ the usual method to do so.
Scene 2.3. *Proving that* $F \subseteq \mathbf{Fix}\,(\mathbf{Gal}\,[K : F])$.
This is trivial by the definition of Galois connection.
Scene 2.4. *Proving that* $\mathbf{Fix}\,(\mathbf{Gal}\,[K : F]) \subseteq F$.
Take any $a \in \mathbf{Fix}\,(\mathbf{Gal}\,[K : F])$. This means that $\forall\ g \in \mathbf{Gal}\,K : F$, $g(a) = a$. We can show that $a \in F$ by somehow showing that for each $k \in K \setminus F$, $\exists f \in \mathbf{Gal}\,K : F$ such that f doesn't fixes k. For this, take any $k \in K \setminus F$ and let $p_k(x) \in F[x]$ be it's minimal polynomial. Clearly, $\deg p_k(x) \geq 2$. Note that $[K : F]$ must be Galois as $[K : P]$ is Galois (Proposition 1.5.2). Since all roots of $p_k(x)$ are distinct and in K, therefore let $k' \neq k \in K$ be some other root of $p_k(x)$. By Proposition 1.4.5, we have an F-automorphism of K which doesn't fixes k.

We have hence proved that $\mathbf{Fix}\,(-) \circ \mathbf{Gal}\,(-) = 1$, proving the final part and hence the whole result. ■

1.6 Galois group of polynomials

We will now aim to prove the insolvability of the quintic polynomial. We follow Section 14.7 of [DF03].

Definition 1.6.1. (**Splitting Field**) *Suppose F is a field and $f(x)$ is a polynomial in $F[x]$. An extension $[K : F]$ of F such that K is the smallest field in which $f(x)$ completely factors linearly is called the splitting field of the polynomial $f(x)$.*

Lemma 1.6.2. Suppose F is a field and $f(x) \in F[x]$ is a separable polynomial. The splitting field of $f(x)$, denoted $[K : F]$, is a Galois extension.

Proof. Suppose $\bar{F}$ is the algebraic closure of base field F and let K be the splitting field of $f(x) \in F[x]$. To show that $[K : F]$ is a Galois extension, we first show that it is algebraic. This is trivial as any $k \in K$ is a linear combination of roots of f (which are algebraic elements) with coefficients from F, and a field generated by algebraic elements is itself algebraic. To show separability, take any $k \in K$ and consider the minimal polynomial of k and write it as $p(x) \in F[x]$. This $p(x)$ would have a root $\beta \in \bar{F}$. We just need to show that $\beta \in K$. It may happen that $f(x)$ would be of degree more than one, but if we can just show that $K = F(\alpha)$ where α is a root of $f(x)$ and then could argue that $[F(\alpha) : F]$ is Galois, then by simple induction we would be done. Therefore WLOG, let us assume that $K = F(\alpha)$ where $\alpha \in \bar{F}$ is a root of $f(x)$. Now, we have a trivial F-isomorphism $\tau : K = F(\alpha) \longrightarrow F(\beta)$ which takes $\alpha \longmapsto \beta$. We want to show that $\beta \in F(\alpha)$. This is simple because τ is an F-isomorphism therefore $f(\beta) = f(\tau(\alpha)) = \tau(f(\alpha)) = \tau(f(\alpha)) = \tau(0) = 0$ and so β is also a root of $f(x)$ and hence $\beta \in F(\alpha)$. Therefore the minimal $p(x) \in F[x]$ has all roots in $F(\alpha) = K$, hence $[K : F]$ is separable. $[K : F]$ is trivially normal as just shown above, where we showed that for each $k \in K$, the minimal polynomial in $F[x]$ has all roots in K. Hence $[K : F]$ is Galois. ∎

Definition 1.6.3. (**Galois Group of a polynomial**) *Suppose F is a field and K is the splitting field of $f(x) \in F[x]$. The Galois group of $f(x)$ is then the Galois group of the extension $[K : F]$, that is,* $\mathbf{Gal}\,[K : F]$.

Definition 1.6.4. (**Elementary Symmetric Functions**) *Let $x_1, \ldots, x_n$ be indeterminates. The elementary symmetric functions $e_k := e_k(x_1, \ldots, x_n)$ is defined as:*

$$e_k(x_1, \ldots, x_n) := \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdot x_{i_2} \cdot \cdots \cdot x_{i_k}.$$

Definition 1.6.5. (n-**degree General Polynomial**) *An n^{th}-degree general polynomial with roots as indeterminates $x_1, \ldots, x_n$ is given as:*

$$(x - x_1) \cdot \cdots \cdot (x - x_n) = \sum_{k=0}^{n} (-1)^k e_k(x_1, \ldots, x_n) x^{n-k}.$$

Remark 1.6.6. Suppose we are working in a base field F and $f(x)$ is an n-degree general polynomial whose roots are indeterminates $x_1, \ldots, x_n$ which are not in F. We then have two extensions of F. First, $F(x_1, \ldots, x_n)$ and second $F(e_1, \ldots, e_n)$. Clearly, by the Definition 1.6.4, we have the following extension:

$$F(x_1, \ldots, x_n) \supset F(e_1, \ldots, e_n).$$

Moreover, this extension is Galois because $F(x_1, \ldots, x_n)$ is the splitting field of the general polynomial $f(x)$ and the rest follows by Lemma 1.6.2

Proposition 1.6.7. Suppose F is a field and $f(x)$ is an n-degree general polynomial. Let S_n act on $\{x_1, \ldots, x_n\}$ and thus on $F(x_1, \ldots, x_n)$. Such actions of S_n is clearly isomorphic to a subgroup G of $\mathbf{Aut}_{F(e_1,\ldots,e_n)}(F(x_1, \ldots, x_n))$ containing those automorphisms of $F(x_1, \ldots, x_n)$ which. We then have that

$$\mathbf{Fix}\,(G) = F(e_1, \ldots, e_n).$$

Proof. The action of S_n on $F(x_1, \ldots, x_n)$ gives those $F(e_1, \ldots, e_n)$-automorphisms of $F(x_1, \ldots, x_n)$ which simply permutes the indeterminates $x_1, \ldots, x_n$. Now, because by above remark, the extension $[F(x_1, \ldots, x_n) : F(e_1, \ldots, e_n)]$ is Galois and finite dimensional, hence by main Galois theorem we have that $\textbf{Fix}\,(\textbf{Gal}\,[F(x_1, \ldots, x_n) :$ is actually $F(e_1, \ldots, e_n)$ itself. Clearly, the group G is just the Galois group of the extension $[F(x_1, \ldots, x_n) : F(e_1, \ldots, e_n)]$ by definition. We hence have our result. ∎

It has a very important corollary:

Corollary 1.6.8. (**Fundamental Theorem of Symmetric Functions**) Suppose $f(x_1, \ldots, x_n)$ is a symmetric function in $\{x_1, \ldots, x_n\}$[8] from $F(x_1, \ldots, x_n)$. Then this $f(x_1, \ldots, x_n)$ is equal to a function in $F(e_1, \ldots, e_n)$.

Proof. Such a symmetric function in $F(x_1, \ldots, x_n)$ clearly is in the fixed field of the subgroup $G \leq \textbf{Aut}_{F(e_1,\ldots,e_n)}(F(x_1, \ldots, x_n))$. By Proposition 1.6.7, $f(x) \in F(e_1, \ldots, e_n)$. ∎

We now prove the important theorem, which characterizes when would the Galois group of a polynomial would be isomorphic to the symmetric group S_n:

Theorem 4. The n-degree general polynomial over the field $F(e_1, \ldots, e_n)$, denoted as:

$$f(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n$$

is separable and has Galois group as S_n.

Proof. The general polynomial $f(x)$ is such that it's coefficients are all indeterminates. Now, if we denote by $x_1, \ldots, x_n$ to be the roots of $f(x)$, then e_i's are elementary symmetric functions of $x_1, \ldots, x_n$. Remember $F(x_1, \ldots, x_n)$ is the splitting field of $f(x)$. We now wish to show that $f(x)$ is separable, that is $x_i \neq x_j$ unless $i = j$. This would follows if we could just show that $\{x_1, \ldots, x_n\}$ are algebraically independent. Suppose $\{x_1, \ldots, x_n\}$ are algebraically dependent. This means that there exists an n variable polynomial $p(t_1, \ldots, t_n) \in F[t_1, \ldots, t_n]$ such that $p(x_1, \ldots, x_n) = 0$. Now, consider $\tilde{p}(x_1, \ldots, x_n) = \prod_{\sigma \in S_n} p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. Clearly, $\tilde{p}$ is a symmetric polynomial and $\tilde{p}(x_1, \ldots, x_n) = 0$. But then we have that $e_1, \ldots, e_n$ is algebraically dependent because this $\tilde{p}$ is a symmetric polynomial in $\{x_1, \ldots, x_n\}$ and thus by Corollary 1.6.8 we have that $\tilde{p}$ is a polynomial in $e_1, \ldots, e_n$ but since $\tilde{p}(x_1, \ldots, x_n) = 0$, therefore this polynomial in $\{e_1, \ldots, e_n\}$ would also be zero, which is a contradiction to the fact that $\{e_1, \ldots, e_n\}$ is algebraically independent. Hence $x_1, \ldots, x_n$ are algebraically independent.

So far we have shown that $f(x)$ is separable, hence it's splitting field is a Galois extension in lieu of Lemma 1.6.2. Now, because of Fundamental Theorem, we have that $\textbf{Fix}\,(\textbf{Gal}\,[F(x_1, \ldots, x_n) : F(e_1, \ldots, e_n)]) = F(e_1, \ldots, e_n)$. But we also have that from Proposition 1.6.7 that $\textbf{Fix}\,(G) = F(e_1, \ldots, e_n)$ where $G \cong S_n$ is the subgroup of automorphisms of $F(x_1, \ldots, x_n)$ which simply permutes the x_i's. By Fundamental Theorem again, we have that $S_n \cong G \cong \textbf{Gal}\,[F(x_1, \ldots, x_n) : F(e_1, \ldots, e_n)]$. Hence the Galois group of $f(x)$ is S_n. ∎

1.7 Solvability and radical extensions

We now study the solvability of a polynomial by radicals and in the process also prove the infamous Abel-Ruffini Theorem.

[8] This means that for any $\sigma \in S_n$, we will have that:

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n).$$

Definition 1.7.1. (**Solvable Groups**) *A group G is solvable if there exists a chain of subgroups:*

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_k = G$$

such that G_i is a normal subgroup in G_{i+1} and quotients G_i/G_{i-1} are cyclic for all $i = 0, \ldots, k-1$.

Definition 1.7.2. (**Galois Closure of an Extension**) *Suppose P is a field and $[F : P]$ is a finite-dimensional separable extension. The Galois closure of the extension $[F : P]$ is then defined as that Galois extension $[K : P]$ where K is the smallest field such that $K \supseteq F$.*

Definition 1.7.3. (**Cyclic Extension**) *A field extension $[K : F]$ is said to be cyclic if the extension is Galois and the corresponding Galois group* **Gal** $[K : F]$ *is cyclic.*

Proposition 1.7.4. Let F be a field with zero characteristic which contains all n^{th}-roots of unity[9]. Then, the extension $[F(\sqrt[n]{a}) : F]$ for any $a \in F$ is a cyclic extension with $\dim[F(\sqrt[n]{a}) : F]$ dividing n.

Proof. To show that $[F(\sqrt[n]{a}) : F]$ is cyclic, we first have to show it is Galois. To this end, because $x^n - a$ is separable and $F(\sqrt[n]{a})$ is the splitting field of $x^n - a$, therefore by Lemma 1.6.2, $[F(\sqrt[n]{a}) : F]$ is a Galois extension. Now, in order to show that **Gal** $[F(\sqrt[n]{a}) : F]$ is cyclic, we will show that it is isomorphic to a subgroup of the group μ_n of n^{th}-roots of unity, which exists for the field F because characteristic of $F \neq 0$. Now, since $\sqrt[n]{a}$ is a root of $x^n - a$, then so is $g(\sqrt[n]{a}) \in F(\sqrt[n]{a})$ where $g \in$ **Gal** $[F(\sqrt[n]{a}) : F]$ because $(g(\sqrt[n]{a}))^n - a = g((\sqrt[n]{a})^n) - a = g((\sqrt[n]{a}) - a) = g(0) = 0$. But we know that the n^{th} roots of a are related multiplicatively by n^{th} roots of unity, therefore we can write $g(\sqrt[n]{a}) = \xi_g \sqrt[n]{a}$ where $\xi_g \in F$ is an n^{th} root of unity. Now, consider the map

$$\begin{aligned} \sigma : \textbf{Gal}\,[F(\sqrt[n]{a}) : F] &\longrightarrow \mu_n \\ g &\longmapsto \xi_g. \end{aligned}$$

We claim that this is an injective homomorphism of groups. Clearly, $\sigma(g \circ h) = \xi_g \cdot \xi_h$ as $\xi_g \in F\ \forall g \in G$, so σ is an homomorphism. It is injective because the kernel of σ, $\ker\sigma$ is clearly the identity of Galois group as only $1 \in$ **Gal** $[F * \sqrt[n]{a} : F]$ is such that $\sigma(1) = 1$ because if g is such that $\sigma(g) = 1$ but $g \neq 1 \in$ **Gal** $[F(\sqrt[n]{a}) : F]$, then $g(\sqrt[n]{a}) = 1 \cdot \sqrt[n]{a} = \sqrt[n]{a}$ which means that g is the identity map of $F(\sqrt[n]{a})$, a contradiction. Hence σ is injective. Therefore **Gal** $[F(\sqrt[n]{a}) : F] \cong \text{Im}\ \sigma \leq \mu_n$ and so $|$**Gal** $[F(\sqrt[n]{a}) : F]|$ divides $|\mu_n| = n$ by Lagrange's theorem and **Gal** $[F(\sqrt[n]{a}) : F]$ is hence cyclic. The proof is complete. ■

The extensions as dealt in Proposition 1.7.4 are called Radical Extensions. We now wish to understand how n^{th} roots of unity and some member a in a field interact. For this we first define the following:

Definition 1.7.5. (**Lagrange Resolvents**) *Suppose $[K : F]$ is a cyclic field extension of dimension n and suppose F is of characteristic 0 and that F contains all n^{th} roots of unity. Let $g \in$* **Gal** $[K : F]$ *be the generator of* **Gal** $[K : F]$*. Then, for any $\alpha \in K$ and any n^{th} root of unity $\xi \in F$, we define the Lagrange resolvent (α, ξ) as the following element of K:*

$$(\alpha, \xi) := \alpha + \xi g(\alpha) + \xi^2 g^2(\alpha) + \cdots + \xi^{n-1} g^{n-1}(\alpha).$$

Remark 1.7.6. The Lagrange resolvent becomes important in an n-dimensional cyclic field extension $[K : F]$ of characteristic 0 because the generator $g \in$ **Gal** $[K : F]$ acts on the resolvent (α, ξ) as follows:

$$\begin{aligned} g((\alpha, \xi)) &= g\left(\alpha + \xi g(\alpha) + \cdots + \xi^{n-1} g^{n-1}(\alpha)\right) \\ &= g(\alpha) + g(\xi g(\alpha)) + \cdots + g(\xi^{n-1} g^{n-1}(\alpha)) \\ &= g(\alpha) + \xi g^2(\alpha) + \cdots + \xi^{n-1} g^n(\alpha) \\ &= g(\alpha) + \xi g^2(\alpha) + \cdots + \xi^{-1} g^n(\alpha) \\ &= \xi^{-1}\left(\xi g(\alpha) + \xi^2 g^2(\alpha) + \cdots + g^n(\alpha)\right) \\ &= \xi^{-1}\left(\xi g(\alpha) + \xi^2 g^2(\alpha) + \cdots + \alpha\right) \\ &= \xi^{-1}(\alpha, \xi). \end{aligned}$$

[9] This means that the polynomial $x^n - 1 \in F[x]$ is normal in F.

Therefore we have

$$(g(\alpha,\xi))^n = (\xi^{-1})^n(\alpha,\xi)^n = (\alpha,\xi)^n$$

which means that $(\alpha,\xi)^n$ is such that $h((\alpha,\xi)^n) = g^m((\alpha,\xi)^n) = (\alpha,\xi)^n \ \forall h = g^m \in \textbf{Gal}\,[K:F]$, which further means that

$$(\alpha,\xi)^n \in \textbf{Fix}\,(\textbf{Gal}\,[K:F]) = F.$$

That is, if $(\alpha,\xi) \in K$ is the Lagrange resolvent of an n-dimensional cyclic extension $[K:F]$, then $(\alpha,\xi)^n \in F$.

We now define the solvability of a polynomial by radicals:

Definition 1.7.7. (**Expression of an Algebraic Element by Radicals**) *Suppose α is an algebraic element over a field F. We say that α can be expressed by radicals if there exists an extension K of F such that $\alpha \in K$ and there are following radical extensions chain to reach to K from F:*

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_k = K$$

where $F_{i+1} = F_i(\sqrt[n]{a_i})$ and $a_i \in F_i$ for all $i = 0, 1, \ldots, k-1$.

Definition 1.7.8. (**Polynomial Solvable in Radicals**) *A polynomial $f(x) \in F[x]$ for a field F is said to be solvable in radicals if each root of $f(x)$ can be expressed by radicals.*

We take for granted the following result:

Proposition 1.7.9. Suppose $\alpha \in K$ is an algebraic element over F and that it is contained in a radical extension of F. Then there exists a radical extension K in which α is expressed, as

$$F = F_0 \subset \cdots \subset F_i \subset \cdots \subset F_k = K$$

$F_{i+1} = F_i(\sqrt[n]{a_i})$ where $a_i \in F_i$, is such that $[K:F]$ is a Galois extension and each $[F_i : F_{i-1}]$ is cyclic.

We now prove when is a polynomial solvable:

Proposition 1.7.10. A polynomial $f(x) \in F[x]$ is solvable in radicals if and only if the Galois group (of it's splitting field) is a solvable group.

Proof. (L $\implies$ R) Suppose $f(x) \in F[x]$ is a polynomial whose all roots α are solvable. By Proposition 1.7.9, there is a field K such that $[K:F]$ is Galois, $\alpha \in K$, there are extensions $F = F_0 \subset \cdots \subset F_k = K$ where F_{i+1} is a radical extension over F_i and $[F_{i+1} : F_i]$ are all cyclic extensions. But this is only for one root α of $f(x)$. Remember that composition of Galois extensions is also a Galois extension. Therefore, for each root α of $f(x)$, let us compose the final fields in which the roots are represented by radicals. Let us denote this composite field (which is Galois) to be L. Again, we have a sequence of radical extensions (by Proposition 1.7.9) $F = K_0 \subset \cdots \subset K_r = L$ where $[K_{i+1} : K_i]$ is cyclic for any i. Now, the Galois group of $f(x)$ is $\textbf{Gal}\,[L:F]$. Let G_i be the subgroups of $\textbf{Gal}\,[L:F]$ which corresponds to the intermediate extensions $[K_i : F]$. Since $[K_i : F]$ is cyclic (and therefore Galois) by Proposition 1.7.9, therefore G_i's are normal subgroups of $\textbf{Gal}\,[K:F]$[10]. With this, we also then have that $\textbf{Gal}\,[K_{i+1} : K_i] = \frac{G_{i+1}}{G_i}$. But this quotient is cyclic by the fact that $[K_{i+1} : K_i]$ is a cyclic extension. Hence the sequence $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r = \textbf{Gal}\,[L:F]$ is such that G_{i+1}/G_i is cyclic and each G_i is normal. Hence $\textbf{Gal}\,[L:F]$, the Galois group of $f(x)$ is solvable.

[10]This requires proof of the fact that intermediate extension $[E:F]$ of a Galois extension $[K:F]$ is Galois if and only if $\textbf{Gal}\,[E:F]$ is normal in $\textbf{Gal}\,[K:F]$. In-fact more is true, that if the preceding is true then, $\textbf{Gal}\,[E:F] = \frac{\textbf{Gal}\,[K:F]}{\textbf{Gal}\,[E:F]}$. However, we haven't proved this for the sake of being concise, which is sad :(.

(R $\implies$ L) Suppose the splitting field of $f(x) \in F[x]$ is $[L : F]$ which is Galois and the Galois group $\textbf{Gal}\,[L : F]$ is solvable. Then there is the sequence $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r = \textbf{Gal}\,[L : F]$ of normal subgroups (G_i is normal in G_{i+1}) and that the quotients G_{i+1}/G_i are cyclic. Corresponding to these G_i's, let us take their fixed fields as follows:

$$F = \textbf{Fix}\,(G_r) \subseteq \cdots \subseteq \textbf{Fix}\,(G_i) \subseteq \cdots \subseteq \textbf{Fix}\,(G_0) = L.$$

Let us denote $F_i := \textbf{Fix}\,(G_i)$. Note that $[F_{i-1} : F_i]$ are cyclic extensions as they are Galois and these quotients of Galois groups are cyclic. Denote also by F' the field obtained by adjoining the F with n_i roots of unity where $i = 0, 1, \ldots, r$. If we then compose F' with all F_i, we get that $F' = F'F_r \subseteq \cdots \subseteq F'F_i \subseteq \cdots \subseteq F'F_0 = F'L =$. Clearly now, $[F'F_{i-1} : F'F_i]$ is cyclic. Now we use an unproved statement that a cyclic extension of dimension n is equal to a radical extension of n^{th} root of some member. Since $[F'F_{i-1} : F'F_i]$ is cyclic, therefore is some $a_i \in F'F_i$ such that $F'F_{i-1} = F'F_i(\sqrt[n_i]{a_i})$. Therefore $F'F_i$ are radical extensions. Hence each root of $f(x)$, which is present in $F'L$, is thus expressed in terms of radical extensions, which means that $f(x)$ is solvable in radicals. ■

Corollary 1.7.11. (**Abel-Ruffini Theorem**) The general polynomial of degree $n \geq 5$ is not solvable in radicals.

Proof. Theorem 4 shows that the n-degree general polynomial has Galois group S_n. But S_n is not solvable for $n \geq 5$. Proposition 1.7.10 then shows that such polynomials cannot be solvable in radicals. ■

2 Grothendieck's Galois theory over commutative algebras

We now start our main investigations of the generalization of Galois theory over fields to now over commutative algebras. We begin with the definition of a commutative algebra:

Definition 2.0.1. (**Commutative Algebra**) *Suppose K is a field and A is a vector space over K. A has the structure of a commutative algebra if A has an additional operation $(- \cdot -)$ which makes A into a commutative ring with identity and the operation of K over A, for any $x, y \in A$ and $c, d \in F$, additionally satisfies*

$$(cx) \cdot (dy) = (cd)(x \cdot y).$$

Remark 2.0.2. Note that for any field K, the ring of polynomials over K, $K[x]$, is a K-algebra.

Definition 2.0.3. (**Ideals in a K-Algebra**) *Suppose K is a field and a ring $(A, +, \cdot)$ is a K-algebra. An ideal I of the K-algebra A is then defined to be an ideal of A as a ring and as a subspace of A as a K-vector space. That is,*

1. *I is a subgroup of abelian group $(A, +)$.*
2. *For any $x \in A$ and any $i \in I$, $x \cdot i \in I$.*
3. *For any $i \in I$ and any $k \in K$, $ki \in I$.*

We now have the following basic properties of K-algebras.

2.1 Properties of K-algebras

First, we see that the quotient of a K-algebra by an ideal is also a K-algebra:

Lemma 2.1.1. Suppose K is a field and A is a K-algebra. Let I be an ideal of A. The quotient ring A/I is then also a K-algebra where the action of K on A/I, for $x + I \in A/I$ and $k \in K$, is given as:

$$(k) \cdot (x + I) = k \cdot x + I.$$

Proof. We first show that the above action of K on A/I is well defined. Suppose $k \cdot (x+I) = k \cdot (y+I)$ where $x+I, y+I \in A/I$. This means that $k \cdot x - k \cdot y = k \cdot (x-y) \in I$. This means that $k^{-1} \cdot k \cdot (x-y) = (x-y) \in I$, and so $x + I = y + I$. Next, to show that this action of K on A/I is indeed such that A/I is a K-algebra, we simply see that $(k \cdot (x+I)) \cdot (k' \cdot (y+I)) = (k \cdot x + I) \cdot (k' \cdot y + I) = (k \cdot x) \cdot (k' \cdot y) + I = (kk') \cdot (x \cdot y) + I = (kk') \cdot ((x + I) \cdot (y + I))$. ■

The kernel of an algebra homomorphism is an ideal:

Lemma 2.1.2. Suppose K is a field with A and B being two K-algebras. Let $f : A \longrightarrow B$ be a K-algebra homomorphism. Then Ker f is an ideal of A.

Proof. Take any $a \in A$ and any $i \in$ Ker f. Clearly then $f(i) = 0$. But now, $a \cdot i \in A$ is such that $f(a \cdot i) = f(a) \cdot f(i) = f(a) \cdot 0 = 0$, hence $a \cdot i \in$ Ker f. ■

An algebra is a field if and only if it has trivial ideals:

Lemma 2.1.3. Suppose K is a field and A is a K-algebra. Then A is a field if and only if A has only trivial ideals.

Proof. (L $\implies$ R) Fields only have trivial ideals.
(R $\implies$ L) If the K-algebra A only has trivial ideals, then for any $a \in A$ which is non-zero, $a \cdot A = A$ as A is a trivial ideal. Therefore, $\exists b \in A$ such that $a \cdot b = 1 \in A$. ■

Surjective K-algebra homomorphisms gives maximal ideals as kernels:

Lemma 2.1.4. Suppose K is a field and A, B are K-algebras. Let $f : A \longrightarrow B$ be a surjective K-algebra homomorphism. If B is a field, then Ker f is a maximal ideal of A.

Proof. By first isomorphism theorem, we have $A/\text{Ker } f \cong \text{Im } f = B$. Let I be an ideal of A such that Ker $f \subset I$. We then have K-algebra homomorphism $\tilde{f} : A/\text{Ker } f \longrightarrow A/I$, which takes $a+\text{Ker } f \longmapsto a+I$. The kernel of $\tilde{f}$ is an ideal of $A/\text{Ker } f \cong B$. But B is a field, so by Lemma 2.1.3, B only has trivial ideals. Ker $\tilde{f}$ is hence a trivial ideal of $A/\text{Ker } f \cong B$. If Ker $\tilde{f} = \{0\}$, then $\tilde{f}(0 + \text{Ker } f) = 0 + \text{Ker } f = 0 + I$, hence Ker $f = I$. Else if Ker $\tilde{f} = A/\text{Ker } f$, then for any $a + \text{Ker } f \in A/\text{Ker } f$, $\tilde{f}(a + \text{Ker } f) = I$, which means that A/I has only one element, that is, $I = A$. Hence, Ker f is either equal to I or I is whole of A, showing that Ker f is maximal. ■

$K[x]$ is a principal K-algebra:

Lemma 2.1.5. Suppose K is a field. Then every ideal of the K-algebra $K[x]$ is principal.

Proof. Take any ideal I of $K[x]$. We wish to find a polynomial in I which generates I. So take the minimal degree $f(x) \in I$ and any $g(x) \in I$. Now, by Euclid's division, there exists $q(x), r(x) \in K[x]$ such that $g(x) = f(x) \cdot q(x) + r(x)$ and $\deg r(x) < \deg f(x)$. Since $f(x) \in I$ and $g(x) \in I$, then $f(x) \cdot q(x) \in I$ and so $r(x) = g(x) - f(x) \cdot q(x) \in I$. But $\deg r(x) < \deg f(x)$ and $f(x)$ is of minimal degree in I, so $r(x) = 0$. This gives us that any $g(x) = f(x) \cdot q(x)$ and hence $f(x)$ generates I. ■

In the K-algebra $K[x]$, the condition of irreducibility can be equivalently stated as follows:

Proposition 2.1.6. Suppose K is a field and $K[x]$ is the K-algebra of polynomials. Let $p(x) \in K[x]$. Then, the following conditions are equivalent:

1. The polynomial $p(x)$ is irreducible in $K[x]$.
2. The generated ideal $\langle p(x) \rangle$ is maximal.
3. The K-algebra $\frac{K[x]}{\langle p(x) \rangle}$ is a field.

Proof. (1) $\implies$ (2) : Take a non-trivial ideal $I \subset K[x]$ such that $\langle p(x) \rangle \subseteq I$. By Lemma 2.1.5, $I = \langle s(x) \rangle$ for some $s(x) \in K[x]$. By Euclid's division in $K[x]$ of $p(x)$ and $s(x)$, we get that $\exists q(x), r(x) \in K[x]$ such that $p(x) = q(x)s(x) + r(x)$ with $0 \leq \deg r(x) < \deg s(x)$. Clearly, $r(x) \in I$, therefore $r(x) = t(x) \cdot s(x)$ for some $t(x) \in K[x]$. But $\deg r(x) < \deg s(x)$ and $\deg t(x) \geq 0$, therefore $r(x) = 0$. Now, $p(x) = q(x) \cdot s(x)$ but $p(x)$ is irreducible, so either $q(x)$ is invertible or $s(x)$ is invertible. Now take any $f(x) \in I$, so we immediately have that $f(x) = u(x) \cdot s(x)$ for some $u(x) \in K[x]$. Now, if $s(x)$ is invertible, then since $s(x) \in I = \langle s(x) \rangle$, hence $s^{-1}(x) \cdot s(x) = 1 \in I$ which thus means that $I = K[x]$ is trivial, but this is not possible as I was taken to be non-trivial. Hence, $q(x)$ is invertible, and so $s(x) = q^{-1}(x) \cdot p(x)$ and hence $f(x) = u(x) \cdot q^{-1}(x) \cdot p(x) \in \langle p(x) \rangle = I$.
(2) $\implies$ (3) : Take any ideal I of $K[x]/\langle p(x) \rangle$ where $\langle p(x) \rangle$ is maximal. Now, remember that we have a K-algebra homomorphism (easy to check) given as:

$$\begin{aligned} \pi : K[x] &\longrightarrow \frac{K[x]}{\langle p(x) \rangle} \\ f(x) &\longmapsto f(x) + \langle p(x) \rangle . \end{aligned}$$

The inverse image $\pi^{-1}(I)$ is an ideal of $K[x]$. But note that since $0_{K[x]/\langle p(x)\rangle} = \langle p(x)\rangle \in I$, therefore $\langle p(x)\rangle \subseteq \pi^{-1}(I)$. But $\langle p(x)\rangle$ is maximal. Therefore, either $\pi^{-1}(I) = K[x]$ or $\pi^{-1}(I) = \langle p(x)\rangle$. If $\pi^{-1}(I) = K[x]$, then $I = K[x]/\langle p(x)\rangle$, which is a trivial ideal. Else if $\pi^{-1}(I) = \langle p(x)\rangle$, then $I = \{0_{K[x]/\langle p(x)\rangle}\}$, which again is a trivial ideal of $K[x]/\langle p(x)\rangle$. Hence any ideal I of $K[x]/\langle p(x)\rangle$ is a trivial ideal. We conclude by Lemma 2.1.3.
(3) $\implies$ (1) : Let $p(x) = a(x) \cdot b(x)$ be a factorization of $p(x)$ in $K[x]$. Clearly, $\langle p(x)\rangle \subseteq \langle a(x)\rangle$. But then, $\langle a(x)\rangle / \langle p(x)\rangle$ is an ideal of $K[x]/\langle p(x)\rangle$ as for any $f(x) + \langle p(x)\rangle \in K[x]/\langle p(x)\rangle$ and $t(x) \cdot a(x) + \langle p(x)\rangle \in \langle a(x)\rangle / \langle p(x)\rangle$, $(f(x) + \langle p(x)\rangle) \cdot (t(x) \cdot a(x) + \langle p(x)\rangle) = f(x) \cdot t(x) \cdot a(x) + \langle p(x)\rangle$. Now, since $K[x]/\langle p(x)\rangle$ is a field, therefore $\langle a(x)\rangle / \langle p(x)\rangle$ is trivial. If $\langle a(x)\rangle / \langle p(x)\rangle = \{\star\}$, then $\langle a(x)\rangle \subseteq \langle p(x)\rangle$ and so $\langle a(x)\rangle = \langle p(x)\rangle$, this means that $a(x)$ and $p(x)$ are associates and so $b(x)$ must be invertible, but K is a field so $b(x)$ must be constant. Else if $\langle a(x)\rangle / \langle p(x)\rangle = K[x]/\langle p(x)\rangle$, then for any $f(x) + \langle p(x)\rangle \in K[x]/\langle p(x)\rangle$, $f(x) + \langle p(x)\rangle = t(x) \cdot a(x) + \langle p(x)\rangle \implies t(x) \cdot a(x) - f(x) \in \langle p(x)\rangle \implies t(x) \cdot a(x) - f(x) = u(x) \cdot p(x) \implies t(x) \cdot a(x) - u(x) \cdot a(x) \cdot b(x) = f(x)$. Let $f(x) = 1$, then, $a(x) \cdot (t(x) - u(x) \cdot b(x)) = 1$, that is $a(x)$ is invertible, so $a(x)$ must be constant. Hence in both cases, the arbitrary factorization of $p(x)$ leads to a trivial factorization of $p(x)$ (one built on units and associates), hence $p(x)$ is irreducible. ■

2.2 Algebraic properties of K-algebras

A field extension $[F : K]$ can equally be viewed as a K-algebra F. Hence, our generalization of the field extensions now identify F and K as different fields, which would lead to Galois theory over K-algebras. As one would have noticed, there should be very little difference between the properties of a field extension $[F : K]$ treated as a vector space or treated as a K-algebra. Hence we quickly state some of the same results as discussed in Section 1.2, but now in context of K-algebras.

Definition 2.2.1. (**Algebraic K-Algebra**[11]) *Suppose K is a field and A is a K-algebra. A is said to be algebraic if*

$$\forall\ a \in A,\ \exists\ \textit{non-zero}\ f(x) \in K[x]\ \textit{such that}\ f(a) = 0.$$

Proposition 2.2.2. Suppose K is a field and A is a K-algebra. If A is of finite dimension as a K-vector space, then A is algebraic.

Proof. Same as Proposition 1.2.3 as in the case of field extensions as a vector space. ■

Definition 2.2.3. (**Minimal Polynomial of an Algebraic Element**) *Suppose A is a K-algebra and $a \in A$ is an algebraic element of A. Then $f_a(x) \in K[x]$ is called the minimal polynomial of $a \in A$ if $f_a(x)$ is the unique least degree polynomial such that it is a factor of (divides) each member of the set $\{g(x) \in K[x] \mid g(a) = 0\}$.*

Remark 2.2.4. Note that we do not require $f_a(x)$ to be irreducible because the argument presented in remark following Definition 1.2.5 that any factorization of the minimal polynomial $f_a(x) = p(x) \cdot q(x)$ would imply that either $p(x)$ or $q(x)$ has a as root holds because there we were working in a field ($p(a)$ and $q(a)$ there would be members of a field), while now we are working in a ring A, where it is not true. So there might be algebraic elements in a K-algebra whose minimal polynomial would happen to be reducible.

However, the following lemma sheds some light when the minimal polynomial would be irreducible:

Lemma 2.2.5. Suppose K is a field and A is a K-algebra with non-zero $a \in A$ being an algebraic element of A. If A is an integral domain, then the minimal polynomial $f_a(x) \in K[x]$ is irreducible.

[11] That's a mouthful!

Proof. Take any non-trivial factorization $f_a(x) = p(x) \cdot q(x)$ in $K[x]$. Since $f_a(a) = 0 = p(a) \cdot q(a)$ and $p(a), q(a) \in A$ where A is an integral domain, therefore either $p(a) = 0$ or $q(a) = 0$, thus implying that there is polynomial of degree lower than that of $f_a(x)$ which has a as a root, thus contradicting the minimality of $\deg f_a(x)$. Hence there are no non-trivial factorizations of $f_a(x)$. ■

The next is an important generalization of the Proposition 1.2.9 to the context of K-algebras, which we will consistently use in the discussion that follows, just like we did back in Section 1:

Proposition 2.2.6. Suppose K is a field and A is a K-algebra with $a \in A$ being an algebraic element of A. Let $f_a(x) \in K[x]$ be the minimal polynomial of $a \in A$ and denote $\deg f_a(x) = n$. The smallest K-subalgebra generated by formal combinations of a, denoted $K(a) \subseteq A$, is isomorphic to[12] (as a K-algebra isomorphism):

$$K(a) \cong \frac{K[x]}{\langle f_a(x) \rangle} = \left\{ k_{n-1}x^{n-1} + \cdots + k_1 x + k_0 + \langle f_a(x) \rangle \mid k_i \in K \, , i = 0, 1, \ldots, n-1 \right\}.$$

Proof. As was the case for fields, $K(a) = \{p(a) \in A \mid p(x) \in K[x]\}$. We take the following K-algebra homomorphism:

$$\begin{aligned} \alpha : \frac{K[x]}{\langle f_a(x) \rangle} &\longrightarrow K(a) \\ p(x) + \langle f_a(x) \rangle &\longmapsto p(a) \end{aligned}$$

where $\deg p(x) \leq n-1$. We first wish to show that α is surjective. For this, take any $p(x) \in K[x]$. By Euclid's division in $K[x]$ of $p(x)$ by $f_a(x)$, we get that there exists $q_1(x), r_1(x) \in K[x]$ such that $p(x) = f_a(x) \cdot q_1(x) + r_1(x)$ where $\deg r_1(x) < \deg f_a(x) = n$. Moreover, $p(a) = f_a(a) \cdot q_1(a) + r_1(a) \implies p(a) = r_1(a)$. Therefore $\alpha\left(r_1(x) + \langle f_a(x) \rangle\right) = r_1(a) = p(a)$, showing that α is surjective.
To show that α is injective, take $p(x) + \langle f_a(x) \rangle, q(x) + \langle f_a(x) \rangle \in K[x]/\langle f_a(x) \rangle$ such that $\deg p(x), \deg q(x) < n$ and $p(a) = q(a)$. We wish to show that $p(x) = q(x)$. Since $(p-q)(x)$ is such that $(p-q)(a) = 0$ and $\deg(p-q)(x) < n$, therefore we have a contradiction to the minimality of $f_a(x)$ with this property. Hence, $(p-q)(x)$ must be trivially zero, i.e. $(p-q)(x) = 0$ and so $p(x) = q(x)$, showing that α is injective. Proof is complete. ■

The following corollary of the above shows that a K-algebra which is an integral domain has inverses of algebraic elements:

Corollary 2.2.7. Suppose K is a field and A is a K-algebra. If A is an integral domain and $a \in A$ is algebraic, then a has an inverse in A.

Proof. Let the K-algebra A be an integral domain and $a \in A$ be algebraic. Then the minimal polynomial $f_a(x) \in K[x]$ is irreducible by Lemma 2.2.5. This means by Proposition 2.1.6 that $K[x]/\langle f_a(x) \rangle$ is a field. But by Proposition 2.2.6, we have that $K[x]/\langle f_a(x) \rangle \cong K(a)$. Hence, corresponding to $a \in K(a)$, there is an element of $p(x) + \langle f_a(x) \rangle \in K[x]/\langle f_a(x) \rangle$ and since $K[x]/\langle f_a(x) \rangle$ is a field, so it's inverse is also present, say $q(x) + \langle f_a(x) \rangle$, which by above K-algebra isomorphism corresponds to inverse $a^{-1} \in K(a)$ of a. ■

We now state the following two important results but without proof:

Proposition 2.2.8. (**Chinese Lemma**) Suppose K is a field and A, B_i for $1 \leq i \leq n$ are K-algebras. Let

$$\{f_i : A \twoheadrightarrow B_i\}_{1 \leq i \leq n}$$

[12]Note that for each equivalence class in $K[x]/\langle f_a(x) \rangle$, there exists a representative polynomial of degree atmost $n-1$ by Euclid's division of any polynomial in the class with $f_a(x)$. This is the reason why we only concern ourselves with representative of degree atmost $n-1$. Also note that $k_i \in K$ could be zero.

be a surjective family of K-algebra homomorphisms. If,

$$\text{Ker } f_i + \text{Ker } f_j = A \; \forall i \neq j,$$

then,

$$\begin{aligned} f : A &\longrightarrow \prod_{1 \leq i \leq n} B_i \\ a &\longmapsto (f_1(a), \ldots, f_n(a)) \end{aligned}$$

is surjective.

And the next is characterization of ideals of the K-algebra K^n:

Proposition 2.2.9. Suppose K is a field and K^n is the K-algebra formed by the direct product of K n-times. Then, any ideal I of K^n is of the form

$$I = \{(k_1, \ldots, k_n) \in K^n \mid k_j = 0 \; \forall \; j \in J\}$$

for some $J \subseteq \{1, \ldots, n\}$.

2.3 Field extension of scalar field

When we had an intermediate extension $[K : F : P]$ as in Section 1, we dealt with F-algebra K and P-algebra K simultaneously. Note here that $F \supseteq P$. Hence to deal with such intermediate extensions in the context of K-algebras (which we have not defined yet), we need to study the effects of field extension of scalars and the interactions it has on the corresponding algebra.
We first note that an intermediate algebra extension is a field:

Proposition 2.3.1. Suppose K is a field and $[L : K]$ is a finite dimensional field extension. If A as in $[L : A : K]$ is an intermediate K-algebra[13], then A is a field.

Proof. Since $[L : K]$ is finite dimensional, hence $[L : K]$ is an algebraic extension (Proposition 2.2.2). If $[L : K]$ is algebraic, then so is $[A : K]$. Also, because L is a field, then A is an integral domain because if it's not, then there are two non-zero elements of A, and thus of L, which when multiplied together gives zero, which is against the fact that L is a field (and so an integral domain). Hence A is an integral domain. But then by Corollary 2.2.7, each element of the K-algebra A has an inverse, so A is a field. ■

Before stating the next important result of this section we have to review tensor product of A-modules where A is a commutative ring.

2.3.1 Tensor product of modules

Definition 2.3.2. (**Bilinear Map**) *Let A be a ring and M, N & H be three A-modules. A map $f : M \times N \longrightarrow H$ is said to bilinear if*

$$\begin{aligned} f_m : N &\longrightarrow H \\ n &\longmapsto f(m, n) \end{aligned}$$

is an A-module homomorphism $\forall \; m \in M$ ***and***

$$\begin{aligned} f_n : M &\longrightarrow H \\ m &\longmapsto f(m, n) \end{aligned}$$

is an A-module homomorphism $\forall \; n \in N$.

[13] It's an intermediate K-algebra NOT an intermediate field!

Definition 2.3.3. (**Tensor Product of two Modules over a Ring**) *Let A be a commutative ring and M & N be two A-modules. The tensor product of M and N over A is defined as the tuple (T, ϕ) where T is another A-module equipped with a bilinear map $\phi : M \times N \longrightarrow T$ which satisfies the following universal property*:

For every A-module L and every bilinear map $f : M \times N \longrightarrow L$, $\exists$ a unique A-module homomorphism $\tilde{f} : T \longrightarrow L$ such that the following commutes:

$$\begin{array}{ccc} T & \xrightarrow{\tilde{f}} & L \\ \uparrow{\scriptstyle \phi} & \nearrow_{f} & \\ M \times N & & \end{array} .$$

T is also denoted by $M \otimes_A N$.

2.3.2 The construction of tensor product over a commutative ring

The following shows the explicit construction of the tensor product, instead the one Definition 2.3.3 gives with respect to the universal property.

Proposition 2.3.4. Let A be a ring and M & N be two A-modules, then the tensor product $M \otimes_A N$ **exists** and is **unique**.

Proof. To show **uniqueness**, take any two (T, ϕ) and (P, ξ) with the universal property given in Definition 2.3.3. Then $\exists$ unique $\tilde{\xi} : T \longrightarrow P$ and $\tilde{\phi} : P \longrightarrow T$ such that $\tilde{\xi} \circ \phi = \xi$ and $\tilde{\phi} \circ \xi = \phi$. Since $\tilde{\xi} \circ \tilde{\phi} \circ \xi = \xi$ and $\tilde{\xi} \circ \tilde{\phi}$ must be unique with this property, therefore $\tilde{\xi} \circ \tilde{\phi} = 1_P$. Similarly, $\tilde{\phi} \circ \tilde{\xi} = 1_T$. Hence $T \cong P$.

Existence of tensor product equivalently just shows how to construct one.
To begin with, construct the free A-module $A^{(M\times N)}$, which is the collection of all formal linear combinations of elements of $M \times N$ with coefficients in A, i.e. for any $c \in A^{(M\times N)}$, $c = \sum_{i=1}^{n} a_i \cdot (x_i, y_i)$ where $x_i \in M, y_i \in N$.
Now, denote the submodule $D \subset A^{(M\times N)}$ which is generated by the elements of $A^{(M\times N)}$ which, if it so happens that there was a bilinear map with co-domain D, then it would map these generating elements to 0. In particular, $D \subset A^{(M\times N)}$ is generated as:

$$D = \langle (x + x', y) - (x, y) - (x', y) \ , \ (x, y + y') - (x, y) - (x, y') \ , \ (a \cdot x, y) - a \cdot (x, y) \ , \ (x, a \cdot y) - a \cdot (x, y) \rangle.$$

After constructing this submodule which is pretty close to *making things bilinear*, to indeed make everything work together perfectly, we just need to *glue together* the D into $A^{(M\times N)}$. That is, we consider now the quotient module

$$T := A^{(M\times N)}/D.$$

Note that each element in T is of the form $(x, y) + D$ where $(x, y) \in A^{(M\times N)}$. Denote this element $(x, y) + D \in T$ as follows:

$$x \otimes y := (x, y) + D \in T.$$

With this, we have the following:

$$\begin{aligned} (x + x') \otimes y &= (x + x', y) + D \\ &= ((x, y) + (x', y)) + D \\ &= (x, y) + D + (x', y) + D \\ &= x \otimes y + x' \otimes y \end{aligned}$$

where the second line holds because $-1 \cdot ((x+x',y)-(x,y)-(x',y)) \in D$, so that $(x,y)+(x',y) \in (x+x',y)+D$.
Similarly, we have:

$$\begin{aligned} x \otimes (y+y') &= x \otimes y + x \otimes y' \\ x \otimes a \cdot y &= a \cdot x \otimes y \\ &= a \cdot (x \otimes y) \end{aligned}$$

Moreover, we clearly have a projection map $\phi : M \times N \longrightarrow T$ given by $(x,y) \longmapsto x \otimes y$ and we can see that it is bilinear:

$$a \cdot \phi_x(y) = a \cdot \phi(x,y) = a \cdot (x \otimes y) = x \otimes a \cdot y = \phi_x(a \cdot y)$$

and similarly for $\phi_y : M \longrightarrow T$. Hence we have a (quotient) module T and a bilinear map $\phi : M \times N \longrightarrow T$. We therefore claim that (T, ϕ) is the required tensor product. To show this, take any A-module L and a bilinear map $f : M \times N \longrightarrow L$. We wish to show that f factors through ϕ uniquely. For this, we first note that such a bilinear map f extends to an unique A-module homomorphism $\tilde{f} : T \longrightarrow L$ as given by:

$$\begin{aligned} \tilde{f} : T &\longrightarrow L \\ x \otimes y &\longmapsto f(x,y) \end{aligned}$$

where clearly $a \cdot \tilde{f}(x \otimes y) = a \cdot f(x,y) = f(a \cdot x, y) = \tilde{f}(a \cdot x \otimes y) = \tilde{f}(a \cdot (x \otimes y))$ and similarly for $+$. Moreover, note that $\tilde{f}(d) = 0 \forall\ d \in D$ as d would be a formal linear combination of the generating elements, where each of such generating elements are mapped to $0 \in L$ by bilinear f. Therefore $\tilde{f}$ is well-defined and hence $\tilde{f} \circ \phi = f$. ■

Remark 2.3.5. (**Tensor Product of K-Algebras**) Hence, for two A-modules M and N, the tensor product $M \otimes_A N$ is an A-module which is given by the collection of elements $x \otimes y \in M \otimes_A N$ where $x \in M$ and $y \in N$ and $x \otimes y := (x,y) + D$ as above. These members $x \otimes y$ has the property that:

$$\begin{aligned} x \otimes (y+y') &= x \otimes y + x \otimes y' \\ (x+x') \otimes y &= x \otimes y + x' \otimes y \\ a \cdot (x \otimes y) &= (a \cdot x) \otimes y \\ &= x \otimes (a \cdot y). \end{aligned}$$

One can then quickly see that if M and N are K-algebras, then their tensor product can be given by considering M and N as K-modules and then constructing the usual module tensor product to form a K-module $M \otimes_K N$ and then, to define $M \otimes_K N$ as a K-algebra, we define the following multiplication; for $x \otimes y, x' \otimes y' \in M \otimes_K N$,

$$(x \otimes y) \cdot (x' \otimes y') = (xx') \otimes (yy')$$

which is valid because M and N are themselves K-algebras. Moreover, this product operation on elements of $M \otimes_K N$ makes it a K-algebra.

2.3.3 Generating new algebra by scalar extension

We now study an important result which would help us in constructing new algebra when we have a scalar field extension of the original algebra. First, we note the following:

Remark 2.3.6. Suppose $[L : K]$ is a field extension, then any L-algebra B is trivially a K-algebra.

Proposition 2.3.7. Suppose $[L : K]$ is a field extension. We then have following:

1. (**L-algebra to K-algebra**) If B is any L-algebra, then B is a K-algebra by restriction.
2. (**K-algebra to L-algebra**) If A is any K-algebra, then $L \otimes_K A$ is an L-algebra, with operations:

$$(l \otimes a) \cdot (l' \otimes a') = (ll' \otimes aa')$$
$$\bar{l}(l \otimes a) = (\bar{l}l) \otimes a$$

for any $l, l', \bar{l} \in L$ and $a, a' \in A$.

More formally, we have the following adjunction between categories **L-Alg** and **K-Alg**, whose objects are L and K-algebras and morphisms are L and K-algebra homomorphisms, respectively[14]:

$$\textbf{K-Alg} \underset{(-)}{\overset{L\otimes_K(-)}{\rightleftarrows}} \textbf{L-Alg} \quad (\perp) .$$

Proof. To show that the above pair $L \otimes_K (-) : \textbf{K-Alg} \rightleftarrows \textbf{L-Alg} : (-)$ is adjoint, we have to show that the following is a natural isomorphism; take any K-algebra A and L-algebra B, we need to show that:

$$\mathrm{Hom}_{\textbf{L-Alg}}(L \otimes_K A, B) \cong \mathrm{Hom}_{\textbf{K-Alg}}(A, B).$$

Isomorphism : Now, take any $f : L \otimes_K A \longrightarrow B$ in **L-Alg**, we have an arrow in **K-Alg** given by $\overline{f} : A \longrightarrow B$ given by $a \longmapsto f(1 \otimes a)$. The fact that this is indeed a K-algebra homomorphism, $\overline{f}(ka) = f(1 \otimes (ka)) = f(k(1 \otimes a)) = kf(1 \otimes a) = k\overline{f}(a)$ for any $k \in K$. Similarly for $+$.
Now, take any arrow $g : A \longrightarrow B$ in **K-Alg**. We then have a map $\overline{g} : L \otimes_K A \longrightarrow B$ given by $(l \otimes a) \longmapsto lg(a)$. This again is an L-algebra homomorphism because $\overline{g}(\bar{l}(l \otimes a)) = \overline{g}((\bar{l}l) \otimes a) = \bar{l}lg(a) = \bar{l}g(la) = \bar{l}g(l \otimes a)$.
Natural : Now, we need to show that the above maps $f \mapsto \overline{f}$ and $g \mapsto \overline{g}$ are natural in A and B. To show this, we take any $f : B \longrightarrow C$ in **L-Alg**, and then we wish to first show that the following commutes:

$$\begin{array}{ccc} \mathrm{Hom}_{\textbf{L-Alg}}(L \otimes_K A, B) & \xrightarrow{\cong} & \mathrm{Hom}_{\textbf{K-Alg}}(A, B) \\ \Big\downarrow{\scriptstyle f\circ -} & & \Big\downarrow{\scriptstyle f\circ -} \\ \mathrm{Hom}_{\textbf{L-Alg}}(L \otimes_K A, C) & \xrightarrow{\cong} & \mathrm{Hom}_{\textbf{K-Alg}}(A, C) \end{array} .$$

To see if this commutes, take any $h : L \otimes_K A \to B$. Then we have to show that $f \circ \overline{h} : A \to C$ in **K-Alg** and $\overline{f \circ h} : A \to C$ in **K-Alg** are same. For this, take any $a \in A$, then $f(\overline{h}(a)) = f(h(1 \otimes a)) = f \circ h(1 \otimes a) = \overline{f \circ h}(a)$. Hence the above diagram commutes.
Next, take any $f : A \longrightarrow D$ in **K-Alg**. We want to see whether the following commutes or not:

$$\begin{array}{ccc} \mathrm{Hom}_{\textbf{L-Alg}}(L \otimes_K A, B) & \xrightarrow{\cong} & \mathrm{Hom}_{\textbf{K-Alg}}(A, B) \\ \Big\uparrow{\scriptstyle -\circ L\otimes_K f} & & \Big\uparrow{\scriptstyle -\circ f} \\ \mathrm{Hom}_{\textbf{L-Alg}}(L \otimes_K D, B) & \xrightarrow{\cong} & \mathrm{Hom}_{\textbf{K-Alg}}(D, B) \end{array} .$$

For this, take any $h : D \to B$. We wish to show that $\overline{h} \circ (L \otimes_K f) = \overline{h \circ f} : L \otimes_K A \to B$. For this, take any $(l \otimes a) \in L \otimes_K A$, then $\overline{h} \circ (L \otimes_K f)(l \otimes a) = \overline{h}(l \otimes f(a)) = lh(f(a)) = l(h \circ f)(a) = \overline{h \circ f}(l \otimes a)$. Hence the above square also commutes. Therefore the above pair of functors are adjoint. ∎

[14] This adjunction is the starting point of the study of classical Galois descent, which we hope to give an account of here.

Corollary 2.3.8. Suppose $[L : K]$ is a field extension and A is a K-algebra. We then have the following (natural) isomorphism:

$$\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) \cong \mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L).$$

Proof. Note that the field L is itself an L-algebra. Rest follows from Proposition 2.3.7. ■

The next result establishes an isomorphism between tensor of quotient algebra with a field extension to the quotient in bigger field:

Proposition 2.3.9. Suppose $[L : K]$ is a field extension and $K[x]$ is viewed as a K-algebra. Let $p(x) \in K[x]$ be any polynomial. We denote $\langle p(x)\rangle_L$ as the ideal generated by $p(x)$ in $L[x]$ when we view $p(x)$ as a member of $L[x]$. Similarly we define $\langle p(x)\rangle_K$. Then, we have the following L-algebra isomorphism:

$$L \otimes_K \frac{K[x]}{\langle p(x)\rangle_K} \cong \frac{L[x]}{\langle p(x)\rangle_L}$$

Proof. We show that the following two L-algebra homomorphisms are inverses of each other:

$$\alpha : L \otimes_K \frac{K[x]}{\langle p(x)\rangle_K} \longrightarrow \frac{L[x]}{\langle p(x)\rangle_L}$$
$$\sum_i^m l_i \otimes (f_i(x) + \langle p(x)\rangle_K) \longmapsto \sum_{i=1}^m l_i f_i(x) + \langle p(x)\rangle_L$$

and

$$\beta : \frac{L[x]}{\langle p(x)\rangle_L} \longrightarrow L \otimes_K \frac{K[x]}{\langle p(x)\rangle_K}$$
$$(l_n x^n + \cdots + l_0) + \langle p(x)\rangle_L \longmapsto \sum_{i=0}^n (l_i \otimes (x^i + \langle p(x)\rangle_K)).$$

α and β are clearly well-defined functions. Moreover, α is clearly an L-algebra homomorphism. Similarly, β is also an L-algebra homomorphism by the property of tensor products.
Now, we wish to show that $\alpha \circ \beta = 1_{L[x]/\langle p(x)\rangle_L}$. For this, take any $\sum_{i=0} l_i x^i + \langle p(x)\rangle_L \in L[x]/\langle p(x)\rangle_L$. We then have

$$\begin{aligned}\alpha \circ \beta \left(\sum_{i=0} l_i x^i + \langle p(x)\rangle_L\right) &= \alpha\left(\sum_{i=0}^n l_i \otimes (x^i + \langle p(x)\rangle_K)\right) \\ &= \sum_{i=0}^n l_i x^i + \langle p(x)\rangle_L\end{aligned}$$

which shows the desiderata. Similarly, we wish to show that $\beta \circ \alpha = 1_{L \otimes_K K[x]/\langle p(x)\rangle_K}$. For this, take any

$l \otimes (f(x) + \langle p(x)\rangle_K) \in L \otimes_K K[x]/\langle p(x)\rangle_K$. We then have:

$$\begin{aligned}
\beta \circ \alpha\,(l \otimes (f(x) + \langle p(x)\rangle_K)) &= \beta\,(lf(x) + \langle p(x)\rangle_L) \\
&= \beta\left(\sum_{i=0}^{n} lk_i x^i + \langle p(x)\rangle_L\right) \\
&= \sum_{i=0}^{n} lk_i \otimes \left(x^i + \langle p(x)\rangle_K\right) \\
&= \sum_{i=0}^{n} k_i \left(l \otimes \left(x^i + \langle p(x)\rangle_K\right)\right) \\
&= \sum_{i=0}^{n} l \otimes \left(k_i x^i + \langle p(x)\rangle_K\right) \\
&= l \otimes \left(\sum_{i=0}^{n} k_i x^i + \langle p(x)\rangle_K\right) \\
&= l \otimes (f(x) + \langle p(x)\rangle_K).
\end{aligned}$$

Hence proved. ■

Remark 2.3.10. (**Zeros in an extension**) Suppose $[L : K]$ is a field extension and $p(x) \in K[x]$. We define $Z_L(p(x)) := \{l \in L \mid p(l) = 0\}$. That is, $Z_L(p(x))$ is the set of all roots of $p(x)$ in extension L.

With the above remark in hand, we then observe that for an extension of scalars, we have a bijection between zeroes of a polynomial in the extension and the collection of all homomorphisms from quotient to the extension:

Proposition 2.3.11. Suppose $[L : K]$ is a field extension and $p(x) \in K[x]$ is any polynomial in the K-algebra $K[x]$. Then there exists a bijection as[15]:

$$Z_L(p(x)) \cong \mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\frac{K[x]}{\langle p(x)\rangle_K}, L\right).$$

Proof. Take the following maps:

$$\begin{aligned}
\alpha : Z_L(p(x)) &\longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\frac{K[x]}{\langle p(x)\rangle_K}, L\right) \\
l &\longmapsto (f(x) + \langle p(x)\rangle_K) \mapsto f(l).
\end{aligned}$$

and

$$\begin{aligned}
\beta : \mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\frac{K[x]}{\langle p(x)\rangle_K}, L\right) &\longrightarrow Z_L(p(x)) \\
\eta : \frac{K[x]}{\langle p(x)\rangle_K} \to L &\longmapsto \eta(x + \langle p(x)\rangle_K)
\end{aligned}$$

where $\eta(x+\langle p(x)\rangle_K)$ is indeed a root of $p(x)$ because $p(\eta(x+\langle p(x)\rangle_K)) = \eta(p(x+\langle p(x)\rangle_K))$ as $p(x) \in K[x]$ and L is a K-algebra and η is a K-algebra homomorphism. Now, $\eta(p(x+\langle p(x)\rangle_K)) = \eta(p(x)+\langle p(x)\rangle_K) = \eta(\langle p(x)\rangle_K) = 0$ as η is a K-algebra homomorphism. So β is well-defined.
Similarly, α is well-defined as $\alpha(l)$ is indeed a K-algebra homomorphism because $\alpha(l)\,(f(x) + \langle p(x)\rangle_K + g(x) + \langle p(x$

[15]This bijection of roots in an extension and the homomorphisms from quotient to extension would be used consistently in future!

$\alpha(l)\left(f(x)+g(x)+\langle p(x)\rangle_K\right)=(f+g)(l)=f(l)+g(l)=\alpha(l)(f(x)+\langle p(x)\rangle_K)+\alpha(l)(g(x)+\langle p(x)\rangle_K)$. Similarly, $k\alpha(l)(f(x)+\langle p(x)\rangle_K)=kf(l)=\alpha(l)(kf(x)+\langle p(x)\rangle_K)$. Hence β is well-defined too.
Now, we wish to show that $\alpha\circ\beta=1_{\mathrm{Hom}_{\textbf{K-Alg}}\left(K[x]/\langle p(x)\rangle_K,L\right)}$. For this, take any $\eta: K[x]/\langle p(x)\rangle_K\to L$, then $\alpha(\beta(\eta))=\alpha(\eta(x+\langle p(x)\rangle_K))=\xi$ where $\xi: K[x]/\langle p(x)\rangle_K\longrightarrow L$ is given by $f(x)+\langle p(x)\rangle_K\longmapsto f(\eta(x+\langle p(x)\rangle_K))=\eta(f(x)+\langle p(x)\rangle_K)$ because η is a K-algebra homomorphism and $f(x)\in K[x]$. Hence $\xi=\eta$, showing that $\alpha\circ\beta(\eta)=1$.
Finally, we wish to show that $\beta\circ\alpha=1_{Z_L(p(x))}$. Take any $l\in Z_L(p(x))$, then $\beta\circ\alpha(l)=\beta(\xi)$ where $\xi:(f(x)+\langle p(x)\rangle_K)\mapsto f(l)$. Now, $\beta(\xi)=\xi(x+\langle p(x)\rangle_K)=l$. Hence $\beta\circ\alpha(l)=l$, proving that α and β give the required isomorphism. ■

We next prove the main theorem of this section which suggests that the algebra homomorphism from algebra to scalar extension are independent elements of the vector space consisting of all vector space homomorphisms from that algebra to extension:

Theorem 5. Suppose $[L:K]$ is a field extension. Let A be any K-algebra and note that L is trivially a K-algebra. Then, the collection

$$\mathrm{Hom}_{\textbf{K-Alg}}(A,L)$$

is independent in the L-vector space of K-linear maps

$$\mathrm{Hom}_{\textbf{K-Vect}}(A,L).$$

Proof. To show the required independence, we instead show that an even bigger set containing $\mathrm{Hom}_{\textbf{K-Alg}}(A,L)$ is independent in an even bigger collection containing $\mathrm{Hom}_{\textbf{K-Vect}}(A,L)$. Namely, we will show that, for any L-algebra B, the collection $\mathrm{Hom}_{\textbf{L-Alg}}(B,L)$ is independent in the L-vector space $\mathrm{Hom}_{\textbf{L-Vect}}(B,L)$. Now, note that, by Corollary 2.3.8, we have $\mathrm{Hom}_{\textbf{K-Alg}}(A,L)\cong\mathrm{Hom}_{\textbf{L-Alg}}(L\otimes_K A,L)$, hence if we let $B=L\otimes_K A$, then our task is to show the independence of $\mathrm{Hom}_{\textbf{L-Alg}}(B,L)$ in the $\mathrm{Hom}_{\textbf{L-Vect}}(B,L)\supset\mathrm{Hom}_{\textbf{K-Vect}}(A,L)$, outlining the strategy.
For this, take any L-algebra B. We first note that any L-algebra homomorphism $f:B\longrightarrow L$ is surjective. To see this, take any $l\in L$, then $l=l\cdot 1=l\cdot f(1)=f(l\cdot 1)$. Hence, by first isomorphism theorem, $B/\mathrm{Ker}\ f\cong\mathrm{Im}\ f=L$. Now, take any two distinct L-algebra homomorphisms $f,g:B\twoheadrightarrow L$. Since $f\neq g$, therefore $\mathrm{Ker}\ f\neq\mathrm{Ker}\ g$ because otherwise for some $b\in\mathrm{Ker}\ f\cap\mathrm{Ker}\ g$ will be such that $f(b)=g(b)=0$, contradicting distinctness of f and g. However, we are not sure whether we can use Chinese Lemma (Proposition 2.2.8) right now or not, mainly because we don't know whether $\mathrm{Ker}\ f+\mathrm{Ker}\ g=B$. But, by Lemma 2.1.4, we can indeed use it, because this that lemma shows that $\mathrm{Ker}\ f$ and $\mathrm{Ker}\ g$ are maximal ideals of B since L is a field, therefore $\mathrm{Ker}\ f+\mathrm{Ker}\ g=B$ because of the obvious facts that (a) sum of two ideals is an ideal, (b) sum of two maximal ideals is a maximal ideal because if it's not, then one of the two ideals will not be maximal, and (c) For any $b\in B$, $b\in\mathrm{Ker}\ f+\mathrm{Ker}\ g$. Let us prove this part (c) ; Take any $b\in B$ such that $b\notin\mathrm{Ker}\ f+\mathrm{Ker}\ g$. Since $f(b)\neq g(b)$ in L as f and g is distinct, hence $f(b)\cdot g(b)=g(f(b)\cdot b)$ and $f(b)\cdot g(b)=f(g(b)\cdot b)$ because f,g are L-algebra homomorphisms. We therefore have $g(f(b)\cdot b)=f(g(b)\cdot b)$. As f and g are distinct, so this can only happen if $f(b)\cdot b=g(b)\cdot b\implies(f(b)-g(b))\cdot b=0$. Since $f(b)-g(b)\neq 0$ and $f(b)-g(b)\in L$, hence $b=0$, that is $b\in\mathrm{Ker}\ f+\mathrm{Ker}\ g$, which is a contradiction. Hence any $b\in B$ is in $\mathrm{Ker}\ f+\mathrm{Ker}\ g$. So we have shown that $B=\mathrm{Ker}\ f+\mathrm{Ker}\ g$.
Now, let $\{f_i:B\twoheadrightarrow L\}_{1\leq i\leq n}$ be a collection of surjective L-algebra homomorphisms which, as shown above, follows $\mathrm{Ker}\ f_i+\mathrm{Ker}\ f_j=B$ when $i\neq j$, and also assume that $\sum_{i=1}^n l_i f_i=0$ for some $l_i\in L$. We now wish to show that $l_i=0$ for all $1\leq i\leq n$. Firstly, by Chinese Lemma, the map

$$\begin{aligned}f:B&\longrightarrow\prod_{1\leq i\leq n}L=L^n\\ b&\longmapsto(f_1(b),\ldots,f_n(b))\end{aligned}$$

is surjective. Secondly, let us assume that $\exists i$ such that $l_i \neq 0$. Then, the following collection

$$S = \left\{ (x_1, \ldots, x_n) \in L^n \mid \sum_{i=1}^{n} l_i x_i = 0 \right\}$$

forms a proper subspace of L^n as it contains $(0, \ldots, 0)$ and is closed under scalar action of L but $(1, \ldots, 1) \notin S$, so it's proper. Moreover, note that for any $(f_1(b), \ldots, f_n(b)) \in \text{Im } f = L^n$, since we have that $\sum_{i=1}^{n} l_i f_i = 0$, hence $\sum_{i=1}^{n} l_i f_i(b) = 0$. This shows that $(f_1(b), \ldots, f_n(b)) \in S$. But this gives us that Im $f \subseteq S \subset L^n$, but we already know that Im $f = L^n$. Hence we have a contradiction to the assumption that $\exists i$ with $l_i \neq 0$. Hence $l_i = 0 \ \forall i = 1, \ldots, n$. This proves the result. ■

Comments on Proof Technique. What we did above was quite nice! We showed independence of a bigger collection as compared to what was given to us to prove. I am wondering how I could've thought of this. One thing I feel that I should have observed first was the surjective nature of a K-algebra homomorphism from a K-algebra A to it's scalar field K. If I would've seen this, then I think it would've clicked in my mind to somehow use Chinese Lemma. After that, everything was quite regular, we showed that the sum of ideals is indeed whole of A and then applied the lemma and then somehow tried to show the independence, that too, in the most obvious way for me, that is by contradiction. Anyways, great proof of a great theorem!

2.4 Splitting algebras

We previously studied splitting field of a polynomial, where the given polynomial completely factors into linear factors. Lemma 1.6.2 additionally shows that such an extension is Galois if the polynomial has no multiple roots. The topic of this section is the exact generalization of it to commutative algebras. The main result of this section is characterizing the conditions equivalent to saying that an algebra could be *split* by a scalar extension.
We first define what we mean by a scalar extension *splitting* the algebra:

Definition 2.4.1. (**Algebra Split by a Scalar Extension**) *Suppose $[L : K]$ is a field extension and A is a K-algebra. A is said to be split by extension field L if:*

1. *A is an algebraic K-algebra.*
2. *For each $a \in A$, the minimal polynomial $f_a(x) \in K[x]$ of a factors completely into linear factors (normality) in $L[x]$ with distinct roots (separability).*

We then define those algebras which are split by the algebraic closure of the scalar field:

Definition 2.4.2. (**Étale Algebra**) *Suppose K is a field and $\overline{K}$ is the algebraic closure[16] of K. Let A be a K-algebra. A is said to be an étale K-algebra if $\overline{K}$ splits A.*

Remark 2.4.3. Note that étale in French means *spread*, which suits the above definition because A is said to be an étale K-algebra if for each $a \in A$, it's minimal polynomial *spreads* into linear factors with distinct roots in the algebraic closure $\overline{K}$.

We now come to an interesting proposition which tells us exactly how do a scalar Galois extension interacts with the trivial algebra structure of the extension itself:

Lemma 2.4.4. Suppose $[L : K]$ is a field extension. Then, $[L : K]$ is a Galois extension if and only if the K-algebra L is split by the extension field L.

[16]Remember, the algebraic closure of a field K is defined to be the algebraic extension L of K as in $[L : K]$ such that each $f(x) \in L[x]$ has **atleast** one root in L.

Proof. (L $\implies$ R) Clearly, the K-algebra L is algebraic as for each $l \in L$, $\exists f_l(x) \in K[x]$ with $f_l(l) = 0$ by the fact that $[L : K]$ is Galois. Moreover, this minimal polynomial $f_l(x)$ is split by L as $[L : K]$ is Galois. (R $\implies$ L) By first point of Definition 2.4.1 , $[L : K]$ is algebraic. By the second point of the same, $[L : K]$ is separable and normal, i.e. Galois. ■

Before stating the main theorem of this section, we quickly define Gelfand Transformation:

Definition 2.4.5. (**Gelfand Transformation**[17]) *Suppose $[L : K]$ is a field extension and A is a K-algebra. Then, the following L-algebra homomorphism is called the Gelfand transformation*[18]*:*

$$\begin{aligned}\mathbf{Gel}\,(-) : L \otimes_K A &\longrightarrow L^{\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L\otimes_k A, L)} := \mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(\mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L \otimes_K A, L\right), L\right)\\ (l \otimes a) &\longmapsto (f \mapsto f(l \otimes a)).\end{aligned}$$

The next result is the main theorem of this section, which characterizes the properties which ensures when a finite dimensional scalar extension splits a finite dimensional algebra:

Theorem 6. Suppose $[L : K]$ is a finite dimensional field extension with $\dim[L : K] = m$ and let A be a finite dimensional K-algebra with $\dim A = n$. Then, the following conditions are equivalent:

1. The field extension L splits K-algebra A.
2. The Gelfand transformation $\mathbf{Gel}\,(-) : L \otimes_K A \longrightarrow L^{\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L\otimes_K A, L)}$ is an L-algebra isomorphism.
3. The following map is an L-algebra isomorphism:
$$\begin{aligned}L \otimes_K A &\longrightarrow L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)}\\ (l \otimes a) &\longmapsto (f \mapsto lf(a)).\end{aligned}$$
4. $\left|\mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L \otimes_K A, L\right)\right| = \dim A = n$.
5. $\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A, L\right)\right| = \dim A = n$.
6. The L-algebras $L \otimes_K A$ and $L^{\dim A}$ are isomorphic to each other.
7. For each $(l \otimes a) \in L \otimes_K A$ with $l \otimes a \neq 0 \otimes 0$, there exists $f \in \mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L \otimes_K A, L\right)$ such that $f(l \otimes a) \neq 0$.

Proof. The proof is long, so we break it down in the following *acts*.

Act 1. *Gelfand Transformation is surjective.*
First note that Gelfand transformation is a surjection because for any $\alpha \in \mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(\mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L \otimes_K A, L\right), L\right)$, since each map $g \in \mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L \otimes_K A, L\right)$ is surjective, so for each $l \in L$, there exists $l \otimes a \in L \otimes_K A$ such that $g(l \otimes a) = l$. Similarly, for that $l \in L$, $\exists g \in \mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L \otimes_K A, L\right)$ such that $\alpha(g) = l$. So if we fix such $l \in L$, then we have g and $l \otimes a$ such that $\alpha(g) = l$ and $g(l \otimes a) = l$. Hence $\mathbf{Gel}\,(l \otimes a)(g) = g(l \otimes a) = l = \alpha(g)$, therefore $\mathbf{Gel}\,(l \otimes a) = \alpha$. Hence $\mathbf{Gel}\,(-)$ is surjective.

Act 2. *The equivalence of conditions 2 to 7.*
(2 $\iff$ 3) By Corollary 2.3.8, we have $\mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L \otimes_K A, L\right) \cong \mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A, L\right)$. The maps which establishes this isomorphism, as given in Proposition 2.3.7, gives the equivalence of statements 2 and 3.

[17] ***IDEA*** This must be a natural transformation between two endofunctors on **L-Alg**. Look at Gelfand Duality $\subset$ Isbell Duality.

[18] The fact that $\mathbf{Gel}\,(-)$ is indeed an L-algebra homomorphism easily follows from the fact that f is itself an L-algebra homomorphism.

($3 \implies 4$) Since $2 \iff 3$, therefore we will prove that $2 \implies 4$. Since Gelfand transformation is an isomorphism, therefore both $L \otimes_K A$ and $L^{\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L)}$ have same dimension as a K-vector space. The dimension of K-algebra $L \otimes_K A$ is mn and the dimension of K-algebra $L^{\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L)}$ is $m \times \left|\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes A, L)\right|$. The last follows from the fact that each vector in the K-algebra $\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L)$ is independent by Theorem 5.
($4 \implies 2$) Since Gelfand transformation is a surjection, also $L \otimes_K A$ and $L^{\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L)}$ have same dimension, so $\mathbf{Gel}(-)$ becomes an isomorphism. We therefore have $2 \iff 4$.
($4 \iff 5$) Again by Corollary 2.3.8, we have $\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L) \cong \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$, which establishes the equivalence.
($5 \implies 6$) Since $2 \iff 4 \iff 5$, therefore we will prove $2 \implies 6$. This is trivial as $L \otimes_K A \cong L^{\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L)}$ means that they have same dimension. Moreover, since $\left|\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L)\right| = \dim A$, so $L^{\mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L)} \cong L^{\dim A}$.
($6 \implies 2$) Since $2 \iff 4 \iff 5 \implies 6$, so $2 \implies 6$, and so if we could prove that $6 \implies 2$, then we would establish $2 \iff 6$ and then we can simply prove $2 \implies 7$ to get $6 \implies 7$. So that's why we are trying to prove $6 \implies 2$. To see $6 \implies 2$, it is enough to prove $6 \implies 4$. To show this, we must show that $\left|\mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L^{\dim A}, L\right)\right| = \dim A$. Theorem 5 shows that $\mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L^{\dim L}, L\right)$ has all independent vectors as L-vector space. Now, the L-vector space $\mathrm{Hom}_{\mathbf{L\text{-}Vect}}\left(L^{\dim A}, L\right)$ is of dimension $\dim A$, the basis being the $\dim A$ projection linear maps. But the same $\dim A$ independent projection maps are also present in the subspace $\mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L^{\dim A}, L\right)$, so to maintain the independence of vectors in $\mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L^{\dim A}, L\right)$, we must have that $\left|\mathrm{Hom}_{\mathbf{L\text{-}Alg}}\left(L^{\dim A}, L\right)\right| = \dim A$.
($6 \implies 7$) As discussed above, we will simply show $2 \implies 7$. Since $\mathbf{Gel}(-)$ is an isomorphism so it must have trivial kernel. Hence, for each non-zero $l \otimes a \in L \otimes_K A$, $\mathbf{Gel}(l \otimes a) : \mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L) \longrightarrow L$ is a non-zero L-algebra homomorphism, so for any $f \in \mathrm{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L)$, $\mathbf{Gel}(l \otimes a)(f) = f(l \otimes a) \neq 0 \in L$.
($7 \implies 2$) We already know that the Gelfand transformation $\mathbf{Gel}(-)$ is a surjection. What condition 7 expresses is exactly that the kernel of $\mathbf{Gel}(-)$ is trivial, hence showing that $\mathbf{Gel}(-)$ is additionally injective to prove that it is an isomorphism.
This completes Act 2.

Act 3. *The conditions 2 to 7 are stable under subobjects, quotients, finite products and tensor products of K-algebra A.*
To show this, we assume that the given K-algebra A of finite dimension $\dim A = n$ follows all conditions from 2 to 7. We will now show that any subobject, quotient, finite product and tensor product of A will also follow the conditions 2 to 7. Since conditions 2 to 7 are equivalent by Act 2, so we just need to show that each of the above construction follows atleast one of the properties mentioned from 2 to 7.
Subobject is stable : Since any subalgebra of A, denoted A_1, will also follow **condition 7**, hence proved.
Quotient is stable : First, take any quotient $A \twoheadrightarrow Q$ of A. We wish to show that the K-algebra Q also satisfies **condition 6**. Remember that quotient is a coequalizer, so it is a colimiting diagram in category **K-Alg**. By Proposition 2.3.7, the tensor product functor $L \otimes_K -$ has a right adjoint. Hence $L \otimes_K -$ preserves small colimits, that is, we have the following quotient in **L-Alg** of $L \otimes_K A$:

$$L \otimes_K A \twoheadrightarrow L \otimes_K Q.$$

Since $L \otimes_K A \cong L^{\dim A}$, so the quotient is $L^{\dim A} \twoheadrightarrow L \otimes_K Q$. The kernel of this quotient is an ideal of $L^{\dim A}$, given by Proposition 2.2.9 as follows:

$$I = \{(l_1, \ldots, l_{\dim A}) \in L^{\dim A} \mid l_j = 0 \ \forall \ j \in J\}$$

for some $J \subseteq \{1, 2, \ldots, \dim A\}$. Since the quotient map is surjective, we have the following by first isomorphism theorem of algebra that $\frac{L^{\dim A}}{I} \cong \frac{L \otimes_K Q}{I} \cong L \otimes_K Q$. Now, $L^{\dim A}/I = \{(l_1, \ldots, l_{\dim A}) + I \mid (l_1, \ldots, l_{\dim A}) \in L^{\dim A}\}$. A member $(l_1, \ldots, l_{\dim A}) + I \in L^{\dim A}/I$ is such a subcollection of $L^{\dim A}$ such that for any $(k_1, \ldots, k_{\dim A}) \in (l_1, \ldots, l_{\dim A}) + I$, $k_i = l_i \ \forall \ i \in J$. Hence, there are $\dim A - |J|$

elements in $L^{\dim A}/I$. So, $L \otimes_K Q \cong \frac{L^{\dim A}}{I} \cong L^{\dim A - |J|}$. To satisfy condition 6, we have to show that $\dim Q = \dim A - |J|$. Since L has dimension m over K and $L^{\dim A}/I$ has dimension $\dim A - |J|$ over L, therefore $L^{\dim A}/I$ has dimension $m \cdot (\dim A - |J|)$ over K. In similar vein, the dimension of $L \otimes_K Q$ over K is $m \cdot \dim Q$. Since $L \otimes_K Q \cong L^{\dim A}/I$, therefore they have same dimension and so $m \cdot \dim Q = m \cdot (\dim A - |J|) \implies \dim Q = \dim A - |J|$.

Finite product is stable : Take another finite dimensional K-algebra B with dimension n' which satisfies conditions 2 to 7. We wish to show that $A \times B$ satisfies **condition 7**. First, we have $L \otimes_K A \cong L^{\dim A}$ and $L \otimes_K B \cong L^{\dim B}$. Since the functor $L \otimes_K - :$ **K-Vect** $\longrightarrow$ **L-Vect** is additive, that is, it is an abelian group homomorphism on homsets, so it preserves finite products. This means that $L \otimes_K (A \times B) \cong (L \otimes_K A) \times (L \otimes_K B) \cong L^{\dim A} \times L^{\dim B} \cong L^{\dim A + \dim B}$. Hence $L \otimes_K (A \times B)$ follows condition 7.

Tensor product is stable : Again, take another finite dimensional K-algebra B with dimension which also satisfies all conditions from 2 to 7. We wish to show that $A \otimes_K B$ also satisfies all conditions from 2 to 7. In order to do this, we will show that $A \otimes_K B$ satisfies the **condition 6**. Since $L \otimes_K A \cong L^{\dim A}$ and $L \otimes_K B \cong L^{\dim B}$, and since tensor product is associative while commuting with finite products as a functor, hence, $L \otimes_K (A \otimes_K B) = (L \otimes_K A) \otimes_K B \cong L^{\dim A} \otimes_K B \cong (L \otimes_K B)^{\dim A} \cong \left(L^{\dim B}\right)^{\dim A} \cong L^{\dim B \cdot \dim A}$. Hence proved.

This completes Act 3.

Act 4. *If A_1, A_2 are subalgebras of A satisfying conditions 2 to 7, then the subalgebra $\langle A_1, A_2 \rangle$[19] will also satisfy conditions 2 to 7.*

We know that the subalgebra $\langle A_1, A_2 \rangle$ is simply

$$\langle A_1, A_2 \rangle = \left\{ \sum_{i=1}^{n} a_i^1 a_i^2 \mid a_i^1 \in A_1 \ , \ \ a_i^2 \in A_2 \right\}.$$

We first note that

$$\begin{aligned} \alpha : A_1 \otimes_K A_2 &\longrightarrow \langle A_1, A_2 \rangle \\ (a_1 \otimes a_2) &\longmapsto a_1 \cdot a_2 \end{aligned}$$

is surjective. Hence by first isomorphism theorem of algebra, we have that $\frac{A_1 \otimes_K A_2}{\operatorname{Ker} \alpha} \cong \langle A_1, A_2 \rangle$. Since Act 3 shows that conditions 2 to 7 are stable under tensor and quotient, hence $A_1 \otimes_K A_2$ satisfies, and hence $\frac{A_1 \otimes_K A_2}{\operatorname{Ker} \alpha}$, satisfies conditions 2 to 7. This completes Act 4.

Act 5. *Field extension L splits A if and only if* $\mathbf{Gel}(-)$ *is an isomorphism.*

(L $\implies$ R) Suppose extension L splits A. Since A is finite dimensional, so by Proposition 2.2.2, A is an algebraic K-algebra. Let $a \in A$ be some member of algebra A such that the degree of it's minimal polynomial $f_a(x)$ is exactly $n =: \dim A$. Let $K(a)$ be the subalgebra of A corresponding to $a \in A$. Since L splits A, so $f_a(x)$ has n roots in L. By Proposition 2.2.6, $K(a) \cong \frac{K[x]}{\langle f_a(x) \rangle}$. By Proposition 2.3.11, we have that $\left| \operatorname{Hom}_{\mathbf{K\text{-}Alg}} \left(\frac{K[x]}{f_a(x)}, L \right) \right| = n$ as there are n roots of $f_a(x)$ in L. Hence, the K-algebra $\frac{K[x]}{\langle f_a(x) \rangle}$ follows condition 5, and so it follows all conditions 2 to 7 by Act 2, in particular, it follows condition 2. This means that $\mathbf{Gel}(-) : L \otimes_K K(a) \longrightarrow L^{\operatorname{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K K(a), L)}$ is an isomorphism. Since $K(a)$ is a subalgebra of A and A is of finite dimension, so if we repeat the above process for finitely many such $a_i \in A$ which has n-degree minimal polynomial, then by Act 4, we would have $\langle K(a_1), \ldots, K(a_m) \rangle = A$, where each of $K(a_1)$ satisfies condition 2, so $\langle K(a_1), \ldots, K(a_m) \rangle$ also satisfies condition 2, giving the conclusion $L \implies R$.

(R $\implies$ L) Suppose $\mathbf{Gel}(-) : L \otimes_K A \longrightarrow L^{\operatorname{Hom}_{\mathbf{L\text{-}Alg}}(L \otimes_K A, L)}$ is an isomorphism. Now, take any $a \in A$ whose minimal polynomial $f_a(x) \in K[x]$ has degree n. Again, by Proposition 2.2.6, we have $K(a) \cong \frac{K[x]}{\langle f_a(x) \rangle}$. Now, $K(a)$ is also a subalgebra of A, where A satisfies condition 2 (hence all 2 to 7). Hence

[19] That is, the subalgebra generated by A_1 and A_2. In other words, the smallest subalgebra of A containing A_1 and A_2.

by Act 3, the subalgebra (subobject) $K(a)$ also satisfies conditions 2 to 7. Now, by condition 5, we have $\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(K(a), L\right)\right| = \dim K(a) = \dim \frac{K[x]}{\langle f_a(x)\rangle} = n$, and so $\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\frac{K[x]}{\langle f_a(x)\rangle}, L\right)\right| = n$. By Proposition 2.3.11, we have $\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\frac{K[x]}{\langle f_a(x)\rangle}, L\right)\right| = |Z_L(f_a(x))|$, so $|Z_L(f_a(x))|$ has n elements, hence each root of $f_a(x)$ is distinct and it linearly factors in L. Hence proved.
Proof is now complete. ■

Comments on Proof Technique. This is another one of the more fascinating theorems, proved in an intriguing way. Let us look at last act, Act 5. As it can be seen there, the usual way of proving that $\mathbf{Gel}\left(-\right)$ is an injective map (surjection is already done by Act 1) is not followed, rather, we look at each subalgebra and see whether it satisfies the isomorphism criterion or not. This is enough because A is finite dimensional, so it can only be generated by finitely many algebras. Hence it is likely that if this non-trivial idea of showing that a *particular* way of generating subalgebras (which would, taken together, would generate whole of A) such that each of which will follow condition 2 (so that A also does), would have come to my mind then perhaps I would have had a shot at cracking it. The $R \implies L$ part in Act 5 uses only subobject stability from Act 4. Moreover, to show that minimal polynomial has all distinct roots in L, they proved that the set of all zeros in L of that minimal polynomial has size exactly the degree of it! This is ingenious! An algebra A of $\dim A = n$ will have elements which will have minimal polynomial of degree n. This follows from the fact that if this is not possible, then for all $a \in A$, it's minimal polynomial $f_a(x) \in K[x]$ will have degree $< n$. Now for $a \neq k \cdot 1$ for some $k \in K$, let $\deg f_a(x) = n - 1$. But then $f_a(a) = 0$, where $1, a, a^2, \ldots, a^{n-1}$ are n independent vectors in A, implies that each coefficient of $f_a(x)$ must be zero, hence giving that this is not possible. The rest of the proof utilizes the previously established facts.

The above theorem concludes this section, where we saw 6 conditions which equivalently characterize when a finite dimensional field extension splits the finite dimensional algebra. In the following, we will use Theorem 6 to establish the general Galois theorem over commutative algebras.

2.5 The Galois theorem over commutative algebras

Let us first revise group actions or G-sets:

Definition 2.5.1. (**G-Sets and morphisms**) *Consider a group G. A G-set is a set X with a left group action of group G. For two G-sets X, Y, a map $f : X \longrightarrow Y$ is said to be a G-set morphism if $f(g \cdot x) = g \cdot f(x)$ for all $g \in G, x \in X$.*

Remark 2.5.2. (**Category of G-sets is a Topos**) For a group G, the category whose objects are G-sets X and G-set morphisms between them is denoted:

$$G - \textbf{Sets}.$$

One may remember from topos theory that $G - \textbf{Sets}$ is an elementary topos, so it has finite limits, finite colimits, a subobject classifier and has exponentials (hence is also cartesian closed). See Chapter 1, [MM92].

First, let us define what we mean by the quotient of the group G by any subgroup (and not just normal subgroups, because we don't wish this quotient to be another group):

Definition 2.5.3. (**Quotient of G by any subgroup**) *Suppose G is a group and $H \leq G$ is a subgroup of G. Then we define G/H as the quotient $G/\sim$ where $\sim$ is the following equivalence relation:*

$$g \sim h \iff g^{-1} \cdot h \in H.$$

Remark 2.5.4. (**Quotient is a G-set**) Let G/H be the quotient of a group G by a subgroup H. Define the following action of group G on G/H:

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g, [x]) &\longmapsto [g \cdot x] \end{aligned}$$

where $[x]$ denotes the equivalence class of $x \in G$ by the quotient relation above. Clearly, this is a group action because it is well-defined and $(1, [x]) \mapsto [1 \cdot x] = [x]$ and $(g \cdot h, [x]) \mapsto [g \cdot h \cdot x] = [g \cdot (h \cdot x)]$. Hence G/H is a G-set.

Now we see that there is no difference (upto bijection) between subgroups of a group G and the quotients of the group G as a G-set:

Proposition 2.5.5. Suppose G is a group, then we have a bijection between subgroups of G and quotients of G-set G, that is,

$$\{H \mid H \leq G\} \cong \{G/\sim \mid \sim \text{ is an equivalence relation on } G.\}.$$

Proof. Let us define $\alpha : \{H \mid H \leq G\} \longrightarrow \{G/H \mid H \leq G\}$, $H \longmapsto G/H$. This is injective because if $G/H = G/J$ for two subgroups $H, J \leq G$, we have that any $[x] \in G/H$ if and only if $[x] \in G/J$, so $x^{-1} \cdot y \in H \iff x^{-1} \cdot y \in J$. Since $[1] \in G/H$, where clearly $[1] = H$, therefore $[1] \in G/J$ and hence $x \in H$ if and only if $x \in J$, so $H = J$. Hence α is injective. Now, take any quotient $Q = G/\sim$ of G. We have the surjection $G \twoheadrightarrow Q$, $x \mapsto [x]$. Therefore $[1] \in Q$. We will show that $[1]$ would be a subgroup of G and $G/[1] \cong Q$. First, take any $x, y \in [1] \subset G$. We wish to show that $x^{-1} \cdot y \in [1]$, which is equivalent to showing that if $x \sim 1$ and $y \sim 1$, then $x^{-1} \cdot y \sim 1$. By symmetry and transitivity, $x \sim y$. Since Q is a G-set by above remark, therefore $g \cdot [x] = [g \cdot x]$. This means that $[x \cdot y] = x \cdot [y]$. Hence $[x^{-1} \cdot y] = x^{-1} \cdot [y] = x^{-1} \cdot [1] = [x^{-1} \cdot 1] = [x^{-1}]$. All that is remaining to be shown is that $[x^{-1}] = [x]$. Since $[1] = [x^{-1} \cdot x] = x^{-1} \cdot [x] = x^{-1} \cdot [1] = [x^{-1}]$, therefore $[x] = [x^{-1}]$. We hence have that $[x^{-1} \cdot y] = [1]$ or $x^{-1} \cdot y \in [1]$. Hence $[1]$ is a subgroup of G. Moreover, for any $[x] \in G/[1]$, we have that $yRx \iff y^{-1} \cdot x \in [1]$, but that is the same relation as that of Q, i.e. $R = \sim$. Hence $Q := G/[1] \cong G/\sim$, or, $\alpha([1]) = Q$. Therefore α is surjective too. Hence α is a bijection. ∎

Remark 2.5.6. Note in the above that it was important for us to consider G as a G-set, otherwise we wouldn't have been able to see why $[x \cdot y] = x \cdot [y]$. So that is why the statement of this proposition explicitly states that "*...a bijection between ... G as a G-set*".

Next result describes that every G-set is a sum of quotients of G-set G:

Proposition 2.5.7. Suppose G is a group and X is a G-set. Then X is isomorphic to a disjoint union of quotients of the G-set G:

$$X \cong \coprod_{i \in I} Q_i.$$

Moreover, when X is finite, then the above sum is finite.

Proof. Let us write $Q_i = G/\sim_i = G/H_i$, where the last equality comes from Proposition 2.5.5. Now take any $x \in X$, then $Gx = \{g \cdot x \in X \mid g \in G\} \subseteq X$. Clearly, Gx is also a G-set. Now define the quotient of G by the following subgroup, $H_x = \{g \in G \mid g \cdot x = h \cdot x \ \forall h \in H_x\}$. This is a subgroup because for $g, h \in H_x$, $g \cdot h^{-1} \cdot (h \cdot x) = g \cdot x$ too. Now, the collection of all such quotients $\{G/H_x\}_{x \in X}$ determine the following map:

$$\begin{aligned} X &\longrightarrow \coprod_{x \in X} G/H_x \\ x &\longmapsto [1]_{H_x} = \{g \in G \mid g \cdot 1 \in H_x\} = H_x \end{aligned}$$

where the coproduct $\coprod_{x \in X} G/H_x$ is the labeled unraveling of the sets G/H_x. Now clearly this map is surjective. For injection, let $y \in X \setminus Gx$. Clearly, $x \neq y$. It is enough to show that $Gx \cap Gy = \emptyset$. For this, suppose that is not true, then $\exists z \in Gx \cap Gy$. Then $z = g \cdot x$ and $z = h \cdot y$ for some $g, h \in G$. Hence $g \cdot x = h \cdot y \iff y = h^{-1} \cdot g \cdot x$. But this means that $y \in Gx$, a contradiction. ■

We now look at the main Galois theorem for commutative algebras:

Theorem 7. (**Fundamental Theorem of Grothendieck's Galois Theory**) Suppose $[K : L]$ is a finite dimensional Galois extension of field K. Denote $\mathbf{Gal}\,[L : K] - \mathbf{Sets}_{\mathrm{Fin}}$ to be the category of finite $\mathbf{Gal}\,[L : K]$ sets and morphisms. Also denote by $\mathbf{Split}_K\,(L)_{\mathrm{Fin}}$ the category of all finite dimensional K-algebras which are split by the extension L and K-algebra morphisms between them[20]. Then, the functor

$$\mathbf{Split}_K\,(L)_{\mathrm{Fin}} \xrightarrow{\mathrm{Hom}_{\mathbf{Split}_K(L)_{\mathrm{Fin}}}(-,L)} \mathbf{Gal}\,[L : K] - \mathbf{Sets}_{\mathrm{Fin}}$$

establishes an **equivalence of categories**. That is,

$$\boxed{\mathbf{Split}_K\,(L)_{\mathrm{Fin}} \equiv \mathbf{Gal}\,[L : K] - \mathbf{Sets}_{\mathrm{Fin}}.}$$

Note that for $A \in \mathbf{Split}_K\,(L)_{\mathrm{Fin}}$, the action of $\mathbf{Gal}\,[L : K]$ on $\mathrm{Hom}_{\mathbf{Split}_K(L)_{\mathrm{Fin}}}(A, L)$ is given as $(g, f) \mapsto g \circ f$ where $g \in \mathbf{Gal}\,[L : K]$ and $f \in \mathbf{Split}_K\,(L)_{\mathrm{Fin}}$. Also note that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) = \mathrm{Hom}_{\mathbf{Split}_K(L)_{\mathrm{Fin}}}(A, L)$ because $\mathbf{Split}_K\,(L)_{\mathrm{Fin}}$ is a full subcategory of $\mathbf{K\text{-}Alg}$.

Proof. We know from Theorem 6 the equivalent conditions for L to split a K-algebra A. We will use the above in conjoint with the relations derived in last two results between a G-set and quotients of G.

Act 1. *If $A \in \mathbf{Split}_K\,(L)_{\mathrm{Fin}}$, then $L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \in \mathbf{Gal}\,[L : K] - \mathbf{Sets}_{\mathrm{Fin}}$, with action being $(g, \psi) \longmapsto$*

[20] So this is a full subcategory of $\mathbf{K\text{-}Alg}$.

$(f \mapsto g(\psi(g^{-1} \circ f)))$.
To prove this, first consider the following action on $L \otimes_K A$:

$$\begin{aligned} \mathbf{Gal}\,[L:K] \times (L \otimes_K A) &\longrightarrow L \otimes_K A \\ (g, l \otimes a) &\longmapsto g(l) \otimes a. \end{aligned}$$

Clearly this is a $\mathbf{Gal}\,[L:K]$-action because $(g, 1 \otimes 1) \mapsto (g(1) \otimes 1) = (1 \otimes 1)$ and $(g \circ h, l \otimes a) \mapsto (g(h(l)) \otimes a)$ which is same as $(g, h(l) \otimes a) \mapsto (g(h(l)) \otimes a)$. Now, by Theorem 6, 3, since L splits A, hence $L \otimes_K A \cong L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}$ via the map:

$$\begin{aligned} \theta : L \otimes_K A &\longrightarrow L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \\ (l \otimes a) &\longmapsto (f \mapsto lf(a)). \end{aligned}$$

Now note that we wish to find what the action of $\mathbf{Gal}\,[L:K]$ on $L \otimes_K A$ transpires to $L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}$ via the above isomorphism. In other words, we wish to find what γ is in the diagram below to make it commute:

$$\begin{array}{ccc} \mathbf{Gal}\,[L:K] \times (L \otimes_K A) & \xrightarrow{\alpha:(g,l\otimes a)\mapsto g(l)\otimes a} & L \otimes_K A \\ \cong \big\downarrow \theta & & \theta \big\downarrow \cong \\ \mathbf{Gal}\,[L:K] \times L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} & \xrightarrow[\gamma]{} & L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \end{array}.$$

Let us take the following candidate for γ:

$$\begin{aligned} \gamma : \mathbf{Gal}\,[L:K] \times L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} &\longrightarrow L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \\ (g, \psi) &\longmapsto \left(f \mapsto g\left(\psi(g^{-1} \circ f)\right)\right). \end{aligned}$$

We just need to show that γ as defined above commutes as in the above diagram. For this, take any $(g, l \otimes a) \in \mathbf{Gal}\,[L:K] \times (L \otimes_K A)$ and let $\psi_{l\otimes a} \in L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}$ be given as $\psi_{l\otimes a}(f) = lf(a)$. We then have:

$$\begin{aligned} \gamma \circ \theta(g, (l \otimes a)) &= \gamma(\theta(g, (l \otimes a))) \\ &= \gamma\left((g, \psi_{l\otimes a})\right) \\ &= g\left(\psi_{l\otimes a}(g^{-1} \circ -)\right) \\ &= g\left(l(g^{-1} \circ -)(a)\right) \\ &= g\left(lg^{-1}((-)(a))\right) \\ &= g(l)g\left(g^{-1}((-)(a))\right) \\ &= g(l)((-))(a) \\ &= g\left(l \cdot (-)(a)\right) \end{aligned}$$

and the other side is

$$\begin{aligned} \theta \circ \alpha((g, l \otimes a)) &= \theta(\alpha(g, l \otimes a)) \\ &= \theta(g(l) \otimes a) \\ &= g(l) \cdot (-)(a) \\ &= g(l \cdot (-)(a)) \end{aligned}$$

Hence the square commutes for this choice of γ, so γ is the required action of $\mathbf{Gal}\,[L:K]$ on $L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}$.

Act 2. *If* $A \in \mathbf{Split}_K(L)_{\mathrm{Fin}}$, *then* $A \cong \mathbf{Fix}\,(L \otimes_K A)$, *where* $\mathbf{Fix}\,(L \otimes_K A) = \{x \in L \otimes_K A \mid \forall g \in$

$\mathbf{Gal}\,[L:K],\ (g\otimes \mathrm{id})(x)=x\}$ *and* $g\otimes \mathrm{id}: L\otimes_K A \longrightarrow L\otimes_K A,\ (l\otimes a)\longmapsto (g(l)\otimes a)$.
Since A is a finite dimensional K-algebra, say $\dim A = n$, then $A\cong K^n$ in **K-Vect**. Now, we reframe our question in terms of K^n. First, because vector spaces are flat, so the tensor product functor preserves finite limits. Hence $L\otimes_K K^n \cong (L\otimes_K K)^n \cong L^n$. Now, take any $g\in \mathbf{Gal}\,[L:K]$. We then clearly have the following commutative diagram:

$$\begin{array}{ccc} L\otimes_K K^n & \xrightarrow{g\otimes \mathrm{id}} & L\otimes_K K^n \\ \cong\downarrow & & \downarrow\cong \\ L^n & \xrightarrow[g^n]{} & L^n \end{array}$$

where the isomorphism $L\otimes_K K^n \longrightarrow L^n$ is given by $(l\otimes(k_1,\ldots,k_n))\longmapsto (lk_1,\ldots,lk_n)$. Hence to show that $A\cong \mathbf{Fix}\,(L\otimes_K A)$, we equivalently show that $\mathbf{Fix}\,(L\otimes_K A)\cong K^n$. Moreover, since $L\otimes_K A\cong L\otimes_K K^n$, hence it is enough to show that $\mathbf{Fix}\,(L\otimes_K K^n)\cong K^n$. To show the latter, we note by the main Galois theorem of classical Galois theory (Theorem 3), we have

$$\begin{aligned}\mathbf{Fix}\,(L\otimes_K K^n) &= \{l\otimes(k_1,\ldots,k_n)\in L\otimes_K K^n \mid \forall g\in \mathbf{Gal}\,[L:K],\ g(l)\otimes(k_1,\ldots,k_n)=l\otimes(k_1,\ldots,k_n)\}\\ &\cong \mathbf{Fix}\,(L^n) := \{(l_1,\ldots,l_n)\in L^n \mid \forall g\in \mathbf{Gal}\,[L:K],\ g(l_i)=l_i\ \forall i=1,\ldots,n\}\\ &\cong (\mathbf{Fix}\,(\mathbf{Gal}\,[L:K]))^n\\ &\cong K^n\cong A.\end{aligned}$$

Hence proved. As a reminder, the map $A\longrightarrow \mathbf{Fix}\,(L\otimes_K A)$ which determines the isomorphism is $a\longmapsto 1\otimes a$.

Act 3. $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(-,L):\mathbf{Split}_K(L)_{\mathrm{Fin}}\longrightarrow_{\mathbf{Gal}\,[L:K]-\mathbf{Sets}_{\mathrm{Fin}}}$ *is full.*
Take any $A,B\in \mathbf{Split}_K(L)_{\mathrm{Fin}}$. We wish to show that for any $\mathbf{Gal}\,[L:K]$-morphism

$$\varphi:\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)\longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)$$

in $\mathbf{Gal}\,[L:K]-\mathbf{Sets}_{\mathrm{Fin}}$, there exists an arrow $\xi:A\longrightarrow B$ such that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(\xi,L)=\varphi$.
So, take any $\mathbf{Gal}\,[L:K]$-morphism φ as above. First, we note that powering with L gives us the following map:

$$\begin{aligned}L^{\varphi}: L^{\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)\right|} &\longrightarrow L^{\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)\right|}\\ (l_f)_{f\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} &\longmapsto (l_{\varphi(h)})_{h\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)}.\end{aligned}$$

We first wish to see whether the above map L^{φ} is in $\mathbf{Gal}\,[L:K]-\mathbf{Sets}_{\mathrm{Fin}}$ or not. For this, take any $(l_f)_{f\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}$ and any $g\in\mathbf{Gal}\,[L:K]$, where action of $\mathbf{Gal}\,[L:K]$ on $L^{\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)\right|}\cong L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}$ and $L^{\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)\right|}\cong L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)}$ is denoted by $\star$ and is given by Act 1. Then,

$$\begin{aligned}L^{\varphi}\left(g\star\left((l_f)_{f\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}\right)\right) &= L^{\varphi}\left((g(l_{g^{-1}\circ f}))_{f\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}\right)\\ &= \left(g(l_{g^{-1}\circ\varphi(h)})\right)_{h\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)}\\ &= \left(g(l_{\varphi(g^{-1}\circ h)})\right)_{h\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)}\end{aligned}$$

whereas the other side is

$$\begin{aligned}g\star L^{\varphi}\left((l_f)_{f\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}\right) &= g\star(l_{\varphi(h)})_{h\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)}\\ &= \left(g(l_{g^{-1}\circ\varphi(h)})\right)_{h\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)}\\ &= \left(g(l_{\varphi(g^{-1}\circ h)})\right)_{h\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)}\end{aligned}$$

Hence, indeed, L^{φ} is a $\mathbf{Gal}\,[L:K]$-morphism.
Now by Theorem 6, 6, we have that $L \otimes_K A \cong L^{\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)\right|}$ and $L \otimes_K B \cong L^{\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)\right|}$. Therefore these isomorphisms provide the following $\mathbf{Gal}\,[L:K]$-morphism $\overline{L^{\varphi}} : L \otimes_K A \longrightarrow L \otimes_K B$ given as in the following diagram:

$$\begin{array}{ccc} L^{\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)\right|} & \xrightarrow{\quad L^{\varphi} \quad} & L^{\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)\right|} \\ \cong\Big| & & \Big|\cong \\ L \otimes_K A & \xrightarrow[\overline{L^{\varphi}}]{} & L \otimes_K B \end{array} .$$

Now, by Act 2 and Theorem 6, 3, we have the following map:

$$\xi : A \cong \mathbf{Fix}\,(L \otimes_K A) \cong \mathbf{Fix}\left(L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}\right) \xrightarrow{L^{\varphi}} \mathbf{Fix}\left(L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)}\right) \cong \mathbf{Fix}\,(L \otimes_K B) \cong B.$$

Our claim is that this arrow $\xi : A \longrightarrow B$ is such that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(\xi, L) = \varphi$. To see this, take any $h \in \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L)$. We now wish to show that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(\xi, L)(h) = h \circ \xi = \varphi(h)$. Loosely speaking, we hence want some term in $h \circ \xi$ so it contains $\varphi(h)$. Now we already have a map for any $h \in \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L)$ as $p_h : L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)} \longrightarrow L$ which maps $(l_f)_{f \in \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)} \longmapsto l_h$. Moreover, note that when we do the following composition $L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \xrightarrow{L^{\varphi}} L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)} \xrightarrow{p_h} L$, we get the following mapping $(l_g)_{g \in \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \longmapsto (l_{\varphi(f)})_{f \in \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)} \longmapsto l_{\varphi(h)}$. We therefore somehow have the term $\varphi(h)$. All we need to do is to get from $l_{\varphi(h)} \in L$ to $\varphi(h) \in \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$, or from $p_{\varphi(h)} : L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \longrightarrow L$ to $\varphi(h) : A \longrightarrow L$. This latter condition can be achieved by noting that the following commutes:

$$\begin{array}{ccc} L \otimes_K A & \xrightarrow[\theta_A]{\cong} & L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \\ {\scriptstyle i_A := 1 \otimes (-)}\uparrow & & \downarrow{\scriptstyle p_{\varphi(h)}} \\ A & \xrightarrow[\varphi(h)]{} & L \end{array} .$$

This commutes because for any $a \in A$ we have $p_{\varphi(h)} \circ \theta_A \circ i_A(a) = p_{\varphi(h)}\left(\theta_A(1 \otimes a)\right) = p_{\varphi(h)}\left((f(a))_{f \in \mathrm{Hom}_{\mathbf{K\text{-}alg}}(A,L)}\right) = \varphi(h)(a)$, so we simply have that $p_{\varphi(h)} \circ \theta_A \circ i_A = \varphi(h)$[21]. This then also holds for any $h \in \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L)$ with it's corresponding i_B, θ_B & p_h.
We summarize the above discussion precisely as follows; consider the above commutative square in conjunction with the following:

$$\begin{array}{ccccc} A & \xrightarrow{i_A} & L \otimes_K A & \xrightarrow[\cong]{\theta_A} & L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \\ {\scriptstyle \xi}\downarrow & & \overline{L^{\varphi}}\downarrow & & \downarrow{\scriptstyle L^{\varphi}} \\ B & \xrightarrow[i_B]{} & L \otimes_K B & \xrightarrow[\theta_B]{\cong} & L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)} \end{array} .$$

The fact that this diagram commutes trivially follows from the chain of compositions in the definition of ξ. In-fact, the above diagram *is* the definition of ξ. The above two diagrams then allow us to do the following inference:

$$\begin{aligned} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(\xi, L)(h) &= h \circ \xi \\ &= (p_h \circ \theta_B \circ i_B) \circ \xi \\ &= p_h \circ \theta_B \circ (i_B \circ \xi) \\ &= p_h \circ \theta_B \circ \overline{L^{\varphi}} \circ i_A \\ &= p_h \circ L^{\varphi} \circ \theta_A \circ i_A \\ &= p_{\varphi(h)} \circ \theta_A \circ i_A \\ &= \varphi(h) \end{aligned}$$

[21] Here θ_A is as described in Act 1.

where we deduced second-to-last line from the previous line from the discussion above. Hence proved.

Act 4. $\mathrm{Hom}_{\textbf{K-Alg}}(-, L) : \textbf{Split}_K(L)_{\mathrm{Fin}} \longrightarrow \textbf{Gal}[L:K] - \textbf{Sets}_{\mathrm{Fin}}$ *is faithful.*
We wish to show that for any $A, B \in \textbf{Split}_K(L)_{\mathrm{Fin}}$ and any $f, g \in \mathrm{Hom}_{\textbf{Split}_K(L)_{\mathrm{Fin}}}(A, B) = \mathrm{Hom}_{\textbf{K-Alg}}(A, B)$, if $\mathrm{Hom}_{\textbf{K-Alg}}(f, L) = \mathrm{Hom}_{\textbf{K-Alg}}(g, L)$, then $f = g$.
So suppose $f, g : A \rightrightarrows B$ are such that $\mathrm{Hom}_{\textbf{K-Alg}}(f, L) = \mathrm{Hom}_{\textbf{K-Alg}}(g, L) : \mathrm{Hom}_{\textbf{K-Alg}}(B, L) \longrightarrow \mathrm{Hom}_{\textbf{K-Alg}}(A, L)$. This means that for any $h \in \mathrm{Hom}_{\textbf{K-Alg}}(B, L)$, we have that $h \circ f = h \circ g$. From Act 3, we have that the following square commutes:

$$\begin{array}{ccc} L \otimes_K B & \xrightarrow{\theta_B} & L^{\mathrm{Hom}_{\textbf{K-Alg}}(B,L)} \\ {\scriptstyle i_B}\uparrow & & \downarrow{\scriptstyle p_h} \\ B & \xrightarrow[h]{} & L \end{array} .$$

So we have that $p_h \circ \theta_B \circ i_B \circ f = p_h \circ \theta_B \circ i_B \circ g$ for all $h \in \mathrm{Hom}_{\textbf{K-Alg}}(B, L)$. Now, remember that $p_h : \prod_{k \in \mathrm{Hom}_{\textbf{K-Alg}}(B,L)} L = L^{\mathrm{Hom}_{\textbf{K-Alg}}(B,L)} \longrightarrow L$ is the projection map for the component corresponding to h, in **K-Alg**.
Now, suppose $\alpha, \beta : X \rightrightarrows \prod_{k \in \mathrm{Hom}_{\textbf{K-Alg}}(B,L)} L$ are *any* arbitrary pair of arrows to the product. We then know that $\alpha = \beta$ if and only if $p_h \circ \alpha = p_h \circ \beta \ \forall h \in \mathrm{Hom}_{\textbf{K-Alg}}(B, L)$. To see this more formally, the (L $\implies$ R) is clearly true. For (R $\implies$ L) part, the hypothesis gives us a unique universal arrow $X \longrightarrow \prod_{k \in \mathrm{Hom}_{\textbf{K-Alg}}(B,L)} L$, the uniqueness then settles the case.
Following the above discussion, we then safely say that $\theta_B \circ i_B \circ f = \theta_B \circ i_B \circ g$. But θ_B is clearly injective and so is i_B. Again, one can see this more formally by noting that $(l_1 f(b_1))_{f \in \mathrm{Hom}_{\textbf{K-Alg}}(B,L)} = (l_2 f(b_2))_{f \in \mathrm{Hom}_{\textbf{K-Alg}}(B,L)}$ means that $l_1 = l_2$ and $b_1 = b_2$ by substituting f for the identity map on non-zero elements of B; we also have that $1 \otimes (b_1 - b_2) = 0$ necessarily implies $b_1 - b_2 = 0$. Hence $\theta_B \circ i_B$ is also injective, and hence $\theta_B \circ i_B \circ f = \theta_B \circ i_B \circ g$ implies $f = g$. Hence proved.

Act 5. $\mathrm{Hom}_{\textbf{K-Alg}}(-, L) : \textbf{Split}_K(L)_{\mathrm{Fin}} \longrightarrow \textbf{Gal}[L:K] - \textbf{Sets}_{\mathrm{Fin}}$ *is essentially surjective.*
Take any $\textbf{Gal}[L:K]$-set X. We wish to show that there exists a K-algebra A split by L such that $\mathrm{Hom}_{\textbf{K-Alg}}(A, L) \cong X$ in $\textbf{Gal}[L:K] - \textbf{Sets}_{\mathrm{Fin}}$.
By Proposition 2.5.7, any such $\textbf{Gal}[L:K]$-set X is isomorphic to coproduct of quotients of $\textbf{Gal}[L:K]$, denoted Q_i, as $X \cong \coprod_{i \in I} Q_i$ [22] where I is finite and where the quotients Q_i of $\textbf{Gal}[L:K]$ corresponds to subgroups H_i of $\textbf{Gal}[L:K]$ as $Q_i = \textbf{Gal}[L:K]/H_i$; this follows from Proposition 2.5.5. Therefore if we could find $A_i \in \textbf{Split}_K(L)_{\mathrm{Fin}}$ such that $\mathrm{Hom}_{\textbf{K-Alg}}(A_i, L) \cong \textbf{Gal}[L:K]/H_i$, then X could be written as $X \cong \coprod_{i \in I} \mathrm{Hom}_{\textbf{K-Alg}}(A_i, L)$ where this coproduct is finite as mentioned before. Such coproducts indeed exists in $\textbf{Gal}[L:K] - \textbf{Sets}_{\mathrm{Fin}}$ as it is a topos. Also note that to show finite (co)products exists, we just need to show that the (co)terminal object and binary (co)products exists. The terminal clearly exists in $\textbf{Split}_K(L)_{\mathrm{Fin}}$ and is given by $\{\star\}$ (the initial being $\emptyset$). We now show the following:

Act 5.1 *: For any* $A, B \in \textbf{Split}_K(L)_{\mathrm{Fin}}$, $\mathrm{Hom}_{\textbf{K-Alg}}(A \times B, L) \cong \mathrm{Hom}_{\textbf{K-Alg}}(A, L) \amalg \mathrm{Hom}_{\textbf{K-Alg}}(B, L)$ *in* $\textbf{Gal}[L:K] - \textbf{Sets}_{\mathrm{Fin}}$.
Two finite G-sets are isomorphic if and only if they have same number of elements. Hence if we wish to show that the $\textbf{Gal}[L:K]$-sets $\mathrm{Hom}_{\textbf{K-Alg}}(A \times B, L)$ and $\mathrm{Hom}_{\textbf{K-Alg}}(A, L) \amalg \mathrm{Hom}_{\textbf{K-Alg}}(B, L)$ are isomorphic, we might as well show that they have same cardinality. This is what we do in the following (we use Theorem 6 and the Act 3 of it's proof, which shows that Theorem 6 is true also for products of K-algebras;

[22] ***IDEA!*** Is $\textbf{Gal}[L:K] - \textbf{Sets}_{\mathrm{Fin}}$ a presentable category? If yes, then can we trace a line from small object argument to trees and to combinatorial model categories?

also note that tensor product functor is left-exact) :

$$\begin{aligned}
\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A\times B,L\right)\right| &\cong \left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L\otimes_K\left(A\times B\right),L\right)\right| \\
&= \left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\left(L\otimes_K A\right)\times\left(L\otimes_K B\right),L\right)\right| \\
&= \left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)}\times L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)},L\right)\right| \\
&= \left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L^{\dim A}\times L^{\dim B},L\right)\right| \\
&= \left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L^{\dim A+\dim B},L\right)\right| \\
&= \dim\left(L^{\dim A+\dim B}\right) \\
&= \dim A+\dim B \\
&= \left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A,L\right)\right|+\left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(B,L\right)\right| \\
&= \left|\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A,L\right)\amalg\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(B,L\right)\right|
\end{aligned}$$

which completes the proof of Act 5.1.

It is hence enough to show that any quotient $\mathbf{Gal}\left[L:K\right]/H\cong\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A,L\right)$ for some $A\in\mathbf{Split}_K\left(L\right)_{\mathrm{Fin}}$. In particular we will claim that for any subgroup $H\leq\mathbf{Gal}\left[L:K\right]$, the quotient

$$\mathbf{Claim}:\ \mathbf{Gal}\left[L:K\right]/H\cong\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\mathbf{Fix}\left(H\right),L\right)$$

where $\mathbf{Fix}\left(H\right)=\left\{l\in L\mid g(l)=l\ \forall g\in H\leq\mathbf{Gal}\left[L:K\right]\right\}$. This is what we shall show in the remaining acts 5.2 to 5.5.

Act 5.2 : $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L,L\right)\cong\mathbf{Gal}\left[L:K\right]$ *in* $\mathbf{Gal}\left[L:K\right]-\mathbf{Sets}_{\mathrm{Fin}}$.
This follows from first noting that any K-algebra endomorphism of L is necessarily a K-endomorphism of L because $f:L\longrightarrow L$ is a K-algebra homomorphism means that $f(k)=f(k\cdot 1)=k\cdot 1=k$, hence f is a K-endomorphism of L. But by Proposition 1.2.12, f must be a K-automorphism. Hence $f\in\mathbf{Gal}\left[L:K\right]$. The reverse inclusion is clear.

Act 5.3 : *The map* $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L,L\right)\longrightarrow\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\mathbf{Fix}\left(H\right),L\right),\ f\longmapsto f|_{\mathbf{Fix}(H)}$ *extends to a quotient map* $\alpha:\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L,L\right)/H\longrightarrow\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\mathbf{Fix}\left(H\right),L\right)$.
Consider the map

$$\begin{aligned}
\alpha:\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L,L\right)&\longrightarrow\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\mathbf{Fix}\left(H\right),L\right) \\
\left(f:L\to L\right)&\longmapsto\left(f|_{\mathbf{Fix}(H)}:\mathbf{Fix}\left(H\right)\to L\right).
\end{aligned}$$

We wish to show that for any $[f]\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L,L\right)/H$, any $h\in[f]$ is such that $f|_{\mathbf{Fix}(H)}=h|_{\mathbf{Fix}(H)}$, so that α is well-defined even in the quotient $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L,L\right)/H$. To see this, remember that $h\in[f]$ means that $f^{-1}\circ h\in H\implies h\in f\circ H\implies h=f\circ g$ for some $g\in H\leq\mathbf{Gal}\left[L:K\right]$. Now, $h|_{\mathbf{Fix}(H)}:\mathbf{Fix}\left(H\right)\longrightarrow L$ is a map which would be same as (as showed above) $(f\circ g)|_{\mathbf{Fix}(H)}:\mathbf{Fix}\left(H\right)\longrightarrow L$. Now, for any $l\in\mathbf{Fix}\left(H\right)$, we have

$$\begin{aligned}
h|_{\mathbf{Fix}(H)}\left(l\right)&=\left(f\circ g\right)|_{\mathbf{Fix}(H)}\left(l\right) \\
&=f\left(g|_{\mathbf{Fix}(H)}\left(l\right)\right) \\
&=f\left(l\right)
\end{aligned}$$

where last line follows because $g\in H$. Hence, $f|_{\mathbf{Fix}(H)}=f|_{\mathbf{Fix}(H)}$. This shows that $\alpha:\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L,L\right)\longrightarrow\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\mathbf{Fix}\left(H\right),L\right)$ safely extends to map $\alpha:\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(L,L\right)/H\longrightarrow\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\mathbf{Fix}\left(H\right),L\right)$, thus completing the proof of Act 5.3.

Act 5.4 : *The map* $\alpha : \text{Hom}_{\textbf{K-Alg}}(L, L)/H \longrightarrow \text{Hom}_{\textbf{K-Alg}}(\textbf{Fix}(H), L)$ *given by* $[f] \longmapsto f|_{\textbf{Fix}(H)}$ *is injective.*
Take any $[f], [h] \in \text{Hom}_{\textbf{K-Alg}}(L, L)/H$ such that $\alpha([f]) = \alpha([h])$. This means that we have $f|_{\textbf{Fix}(H)} = h|_{\textbf{Fix}(H)}$. We wish to show that $[f] = [h]$. For this, we just have to show that $f \in [h]$ and so that $f^{-1} \circ h \in H \implies h \in f \circ H$. We hence wish to show that $\exists g \in H$ such that $h = f \circ g$ or $f^{-1} \circ h = g$. To see this, let us compute $f^{-1} \circ h : L \longrightarrow L$. We see that for $l \in \textbf{Fix}(H) \subseteq L$, we have $f^{-1} \circ h(l) = f^{-1}(h(l)) = f^{-1}(f(l)) = l$ where second-to-last equality follows from the given fact that $f|_{\textbf{Fix}(H)} = g|_{\textbf{Fix}(H)}$. Hence $f^{-1} \circ h$ fixes each member of $\textbf{Fix}(H) \subseteq L$. This means that $f^{-1} \circ h \in \textbf{Gal}[L : \textbf{Fix}(H)]$. But by classical Galois theorem (Theorem 3), we have that $\textbf{Gal}[L : \textbf{Fix}(H)] = H$, hence $f^{-1} \circ h \in H$, completing the proof of Act 5.4.

Act 5.5 : *The map* $\alpha : \text{Hom}_{\textbf{K-Alg}}(L, L)/H \longrightarrow \text{Hom}_{\textbf{K-Alg}}(\textbf{Fix}(H), L)$ *given by* $[f] \longmapsto f|_{\textbf{Fix}(H)}$ *is surjective.*
Take any K-algebra homomorphism $g : \textbf{Fix}(H) \longrightarrow L$. Note that we have an intermediate K-algebra $L \supseteq \textbf{Fix}(H) \supseteq K$. By Proposition 2.3.1, $\textbf{Fix}(H)$ is an intermediate field. Also by Proposition 1.5.2, $[L : \textbf{Fix}(H)]$ is a Galois extension. Moreover by Lemma 2.4.4, K-algebra $L \supseteq \textbf{Fix}(H)$ is split by $[L : \textbf{Fix}(H)]$, that is $\textbf{Fix}(H) \in \textbf{Split}_K(L)_{\text{Fin}}$. Finally, by Proposition 1.4.4, the K-homomorphism $g : \textbf{Fix}(H) \longrightarrow L$ extends to a K-automorphism $\bar{g} : L \longrightarrow L$ so that $\bar{g}|_{\textbf{Fix}(H)} = g$, that is $\alpha(\bar{g}) = g$. This completes the proof of Act 5.5 and hence of Act 5.

The proof of Theorem 7 is now complete. ■

The following corollary is exactly the claim after Act 5.1, but is important enough to stand on it's own:

Corollary 2.5.8. Let $[L : K]$ be a finite dimensional Galois extension and let $H \leq \textbf{Gal}[L : K]$ be a subgroup. Then,

$$\textbf{Gal}[L : K]/H \cong \text{Hom}_{\textbf{K-Alg}}(\textbf{Fix}(H), L).$$

Proof. Act 5.2 to 5.5 of proof of Theorem 7. ■

Remark 2.5.9. (**Classical Galois Theorem inside Grothendieck's Galois Theorem**) The Theorem 7 is the general Galois theorem on commutative algebras. However, it should be expected that the classical Galois theorem (Theorem 3) follows from it if we ought to say that Theorem 7 *generalizes* Theorem 3. This is exactly what we shall see now.
Theorem 3 establishes an isomorphism between subgroups of Galois group and intermediate extensions. Take any intermediate extension $L \supseteq F \supseteq K$. Theorem 7 says that $\text{Hom}_{\textbf{K-Alg}}(-, L) : \textbf{Split}_K(L)_{\text{Fin}} \longrightarrow \textbf{Gal}[L : K] - \textbf{Sets}_{\text{Fin}}$ is full, faithful & essentially surjective. Therefore, the extensions $L \supseteq F \supseteq K$ are taken to

$$\textbf{Gal}[L : K] \cong \text{Hom}_{\textbf{K-Alg}}(L, L) \xrightarrow{-\circ\iota_{FL}} \text{Hom}_{\textbf{K-Alg}}(F, L) \xrightarrow{-\circ\iota_{KF}} \text{Hom}_{\textbf{K-Alg}}(K, L) = \{\star\}.$$

Clearly, $-\circ\iota_{FL}$ and $-\circ\iota_{KF}$ are surjective mappings where $-\circ\iota_{FL}$ is surjective in particular by Proposition 1.4.4. Now, by first isomorphism theorem, we will have $\textbf{Gal}[L : K]/\text{Ker}(-\circ\iota_{FL}) \cong \text{Hom}_{\textbf{K-Alg}}(L, L)/\text{Ker}(-\circ\iota_{FL}) \cong \text{Hom}_{\textbf{K-Alg}}(F, L)$ and $\text{Hom}_{\textbf{K-Alg}}(F, L)/\text{Ker}(-\circ\iota_{KF}) \cong \text{Hom}_{\textbf{K-Alg}}(K, L) = \{\star\}$. The main thing to note here is the following quotient isomorphism:

$$\textbf{Gal}[L : K]/\text{Ker}(-\circ\iota_{FL}) \cong \text{Hom}_{\textbf{K-Alg}}(F, L).$$

By Proposition 2.5.5, the quotient $\textbf{Gal}[L : K]/\text{Ker}(-\circ\iota_{FL})$ is isomorphic to some subgroup of $\textbf{Gal}[L : K]$, say H. Therefore $H \cong \text{Hom}_{\textbf{K-Alg}}(F, L)$.
Similarly, for any subgroup of $H \leq \textbf{Gal}[L : K]$, from Theorem 7, we have the quotient $\textbf{Gal}[L : K]/H$ present in $\textbf{Gal}[L : K] - \textbf{Sets}_{\text{Fin}}$. We then have the intermediate extension (by Proposition 2.3.1) $\textbf{Fix}(H) \in \textbf{Split}_K(L)_{\text{Fin}}$ such that $\text{Hom}_{\textbf{K-Alg}}(\textbf{Fix}(H), L) \cong \textbf{Gal}[L : K]/H$ (by Acts 5.4 & 5.5 of the proof of Theorem 7). This proves the inclusion of classical Galois theorem in the Grothendieck's Galois theorem.

3 Infinite dimensional Grothendieck's Galois theory

What we have seen so far is first the classical Galois theory culminating in Theorem 3 and then it's generalization to Grothendieck's Galois theory as in Theorem 7. One common theme in both these theorems were the requirement of finite-dimensional Galois extension (additionally of that of finite dimensional algebra in Theorem 7). We will now see how to get rid of the constraint of finite dimensionality of the Galois extension. Developing this would take us through the realization that the Galois group in this case comes with a natural topology on it, and the fundamental theorem will accordingly say about the connection between the closed sets of this space and intermediate extensions. But we will be more general than this as we will first see the theory for non-finite dimensional commutative algebras, and the fundamental theorem here would then provide as a special case the fundamental theorem for non-finite dimensional Galois field extensions.

3.1 Profinite & totally disconnected spaces

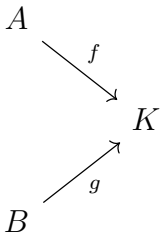
We shall soon see that the category of profinite spaces with Galois group action replace the $\mathbf{Gal}\,[L:K]-\mathbf{Sets}_{\mathrm{Fin}}$ in Theorem 7 when we let go of restriction of finite dimensionality (in K-algebras and in Galois group both). Hence, in order to prove such a result, we need a good understanding of profinite topological spaces, which we start accumulating now.

> ***Main goal of this section :*** We wish to establish the following result: A space is profinite if and only if it is totally disconnected and compact, Theorem 8.

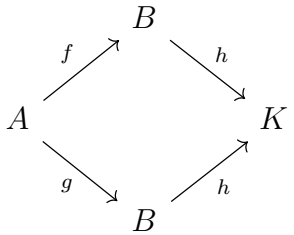
We first look at (co)filtered categories (a general reference is Chapter 9, [Mac78]):

Definition 3.1.1. (**Filtered Categories**) *A non-empty category* $\mathbf{J}$ *is filtered when*

1. *For any two objects* A *and* B *in* $\mathbf{J}$*, there exists an object* K *and arrows* $f : A \to K$ *and* $g : B \to K$*. In diagrammatic terms, this means:*



2. *For any parallel pair of arrows* $f, g : A \rightrightarrows B$ *in* $\mathbf{J}$*, there exists an object* K *and an arrow* $h : B \to K$ *such that the following commutes:*



to yield that $h \circ f = h \circ g$*.*

Remark 3.1.2. (**J is filtered iff each finite diagram has a cocone**) This is simple to see, as if each diagram in $\mathbf{J}$ has a cocone then Definition 3.1.1 follows trivially, and if $\mathbf{J}$ is filtered, then, since each cocone is made up of diagrams exactly that portrayed in Definition 3.1.1[23], therefore any finite diagram has a cocone.
We will hence use this as a more tenable definition of filtered categories.

[23] Remember how finite colimits are made by initial objects, binary coproducts & coequalizers.

Remark 3.1.3. (**Cofiltered Categories**) This is the dual notion of Definition 3.1.1. A category **J** is cofiltered if and only if each diagram in it has a cone. The poset $(\mathbb{N}, \geq)$ is **cofiltered** because for any subset $S \subset \mathbb{N}$ has a lower bound (cone) in $\mathbb{N}$.

Definition 3.1.4. (**Projective System and Limit**) *Suppose* $\mathbf{C}$ *is a category. and* $D : \mathbf{J} \longrightarrow \mathbf{C}$ *is a diagram in* $\mathbf{C}$. *We call* D *a projective system if* $\mathbf{J}$ *is a cofiltered poset. The limit of such a diagram* D *is called a projective limit.*

Remark 3.1.5. Therefore a projective system in a category $\mathbf{C}$ guarantees that there would be a cone for that system in $\mathbf{C}$. Projective limit hence refers to the universal cone for that system.

Let us now explain the limit of a diagram in **Top**:

Lemma 3.1.6. Suppose $D : \mathbf{J} \longrightarrow \mathbf{Top}$ is a diagram in **Top**. The limiting space $\varprojlim D$ is given by the following:

$$\varprojlim D \cong \left\{ (x_i)_{i \in Ob(\mathbf{J})} \in \prod_{i \in Ob(\mathbf{J})} Di \mid \forall Df : Di \longrightarrow Dj,\ \forall f : i \to j \in Ar\left(\mathbf{J}\right),\ f(x_i) = x_j \right\}$$

which has the subspace topology of $\prod_{i \in I} X_i$.

Proof. To see that the subspace, say S, of $\prod_{i \in Ob(\mathbf{J})} Di$ as defined above is indeed the limiting space of the diagram D, we check whether it follows the universal property of being a limit. For this, consider X is a space such that it has maps $\{\alpha_i : X \longrightarrow Di\}_{i \in Ob(\mathbf{J})}$ such that it forms a cone over D. We then have a map $\tau : X \longrightarrow S$ given by $x \longmapsto (\alpha_i(x))_{i \in Ob(\mathbf{J})}$. Clearly, for any $\alpha_i : X \longrightarrow Di$, we have that $\alpha_i(x) = \pi_i(\tau(x))$ where π_i is the projection to i^{th} coordinate (note that these projections form the components of the limiting cone). Hence each α_i factors via τ and so S as defined is indeed isomorphic to $\varprojlim D$. ■

We are now ready to state the definition of a profinite space:

Definition 3.1.7. (**Profinite Topological Space**) *Suppose* **Top** *is the category of topological spaces and continuous maps and* $\mathbf{Top}^{\mathrm{Dscrt}}_{\mathrm{Fin}}$ *is the full-subcategory of* **Top** *of all finite discrete topological spaces and continuous maps. Let* $\iota : \mathbf{Top}^{\mathrm{Dscrt}}_{\mathrm{Fin}} \hookrightarrow \mathbf{Top}$ *be the inclusion functor. A topological space* X *in* **Top** *is called profinite if there exists a cofiltered poset* $\mathbf{J}$ *and a projective system/diagram* $D : \mathbf{J} \longrightarrow \mathbf{Top}^{\mathrm{Dscrt}}_{\mathrm{Fin}}$ *such that* $X \cong \varprojlim(\iota \circ D)$ in **Top**. *That is,* X *is a* ***pro****jective limit of discrete* ***finite*** *spaces.*

Lemma 3.1.6 will be used to analytically explain this profinite space as the projective limit of it's system. We next look at totally disconnected space:

Definition 3.1.8. (**Totally Disconnected Topological Space**) *Suppose* X *is a topological space and* $x, y \in X$ *are any two distinct points in it. If there exists closed & open sets* $U, V \subseteq X$ *with* $U \cap V = \emptyset$ *such that* $x \in U$, $y \in V$, *then* X *is said to be totally disconnected.*

Remark 3.1.9. (**Totally Disconnected** $\implies$ **Hausdorff**) This is quite trivial to see.

The following is an easy consequence of the definition of totally disconnected spaces:

Lemma 3.1.10. A topological space X is totally disconnected if and only if the only connected subspaces of X are singletons.

Proof. (L $\implies$ R) Let X be totally disconnected and take any connected subspace $Y \subseteq X$. We wish to show that Y is a singleton set. The contrapositive here to prove is that Y is just a non-singleton subspace and then we wish to prove that Y is disconnected. This is easy since $Y = \{a, b, \dots\}$ and since $Y \subseteq X$ where X is totally disconnected, hence Y is also totally disconnected. Then Y is disconnected as for (any)

$a \in Y$, there exists a clopen $a \in U \cap Y$, and so $U^{\complement} \cap Y$ is clopen and so they form a separation of Y, making Y disconnected.
(R $\implies$ L) Given is the fact that only singletons are connected in X. We have to show that X is totally disconnected. Suppose it is not true, this means that the only connected subspaces of X are singletons but X is not totally disconnected. The latter that there is a pair of point $x, y \in X$ such that there are no disjoint clopen sets containing x and y, respectively. But then $\{x, y\} \subset X$ would become connected as there would be no separation of $\{x, y\}$, which is a contradiction to the former fact that X has only singletons as connected. Hence proved. ■

We now start to look at some of the fundamental results on profinite spaces which would prove to be helpful to us in our pursuit of proving the said equivalence as mentioned in the beginning of this section. The main theorem in this section will give us a characterization of profinite spaces in terms of compact & totally disconnected spaces.

We first begin by noting that a projective limit of totally disconnected spaces is again totally disconnected:

Proposition 3.1.11. Suppose **Top** is the category of topological spaces and continuous maps. Let $\{X_i\}_{i \in I}$ be a projective system in **Top** of totally disconnected spaces. Then the projective limit $\varprojlim_{i \in I} X_i$ is also a totally disconnected space.

Proof. If we can show that the product space $\prod_{i \in I} X_i$ is also totally disconnected, then, since any subspace of a totally disconnected space is also totally disconnected, we would be done as $\varprojlim_{i \in I} X_i \subseteq \prod_{i \in I} X_i$. Hence our first objective is to try to see if $\prod_{i \in I} X_i$ is also totally disconnected. For this, take any two distinct $(x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} X_i$. We wish to find clopen disjoint sets in $\prod_{i \in I} X_i$ such that each of them contains one of the points. For each $i \in I$, since X_i is totally disconnected, hence $\exists$ disjoint clopen $U_i, V_i \subseteq X_i$ such that $x_i \in U_i$, $y_i \in V_i$. We then have that $\prod_{i \in I} U_i, \prod_{i \in I} V_i \subseteq \prod_{i \in I} X_i$ which are both clopen and disjoint; they are clopen because $\left(\prod_{i \in I} U_i\right)^{\complement} = \prod_{i \in I} U_i^{\complement}$ which is also open as each $U_i^{\complement}$ is open, similarly for $\prod_{i \in I} V_i$ is also clopen. Moreover, $(x_i)_{i \in I} \in \prod_{i \in I} U_i$ and $(y_i)_{i \in I} \prod_{i \in I} V_i$. Hence $\prod_{i \in I} X_i$ is also totally disconnected. Hence the subspace $\varprojlim_{i \in I} X_i \subseteq \prod_{i \in I} X_i$ is also totally disconnected. ■

We next see that the projective limit of compact totally disconnected spaces is also compact totally disconnected:

Proposition 3.1.12. Suppose $\{X_i\}_{i \in I}$ is a projective system in **Top** of compact & totally disconnected spaces. Then the projective limit $\varprojlim_{i \in I} X_i$ is also a compact & totally disconnected space.

Proof. The total disconnectedness of $\varprojlim_{i \in I} X_i$ is clear from Proposition 3.1.11. If we could then show that the projective limit of a compact Hausdorff space is also compact and Hausdorff, then we would be done. By the famous Tychonoff theorem, the product space $\prod_{i \in I} X_i$ is also compact, and it is trivially Hausdorff. Now, we recall a easy to see result that a closed subspace of a compact space is also compact. So now if we could show that $\varprojlim_{i \in I} X_i \subseteq \prod_{i \in I} X_i$ is closed, then we would be done. So we will now show that $\varprojlim_{i \in I} X_i$ is indeed closed. For this, we first note that $\varprojlim_{i \in I} X_i$ is Hausdorff because $\prod_{i \in I} X_i$ is Hausdorff and the former is it's subspace. Finally, we show that $\varprojlim_{i \in I} X_i$ contains all it's limit points, hence making it closed. So take any $(x_j)_{j \in I} \in \prod_{j \in I} X_j$ which is a limit point of $\varprojlim_{i \in I} X_i$. Hence for any open set $(x_j)_{j \in I} \in \prod_{j \in I} U_j \subseteq \prod_{j \in I} X_j$, we must have that $\prod_{j \in I} U_j \setminus \{x_j\} \cap \varprojlim_{i \in I} X_i \neq \emptyset$. This can only happen if $U_j \setminus \{x_j\} \cap \pi_j(\varprojlim_{i \in I} X_i) \neq \emptyset$. Now let's focus attention to space X_j. Assume that $x_j \notin U_j$. Since X_j is Hausdorff, therefore $\exists$ open $V_j \subseteq X_j$ such that $x_j \in V_j$ and $V_j \cap \pi_j(\varprojlim_{i \in I} X_i) = \emptyset$. This gives us an open set $V_j \subseteq X_j$ for each $j \in J$. Hence $\prod_{j \in I} V_j \subseteq \prod_{i \in I} X_i$ is an open set which contains $(x_j)_{j \in I}$ but doesn't intersect $\varprojlim_{i \in I} X_i$. This gives us a contradiction as $(x_j)_{j \in I}$ is a limit point of $\varprojlim_{i \in I} X_i$. Hence our assumption that $(x_j)_{j \in I} \notin \varprojlim_{i \in I} X_i$ is wrong and so $\varprojlim_{i \in I} X_i$ is closed, completing the proof. ■

We next have the following important result on profinite spaces, which says that a space is profinite if and only if it is totally disconnected & compact:

Theorem 8. Let X be a topological space. X is profinite if and only if it is compact & totally disconnected.

Proof. (L $\implies$ R) Let X be profinite, so that there is a projective system of finite discrete spaces $\{X_i\}_{i\in I}$ whose limit $\varprojlim_{i\in I} X_i \cong X$. Now note that a space which is finite and discrete is trivially a totally disconnected space as each neighborhood is clopen in it (in particular, singletons). Moreover, any such finite discrete space is compact too as it is finite; for each $x \in X_i$, take an open neighborhood of x and then take union of all such for each $x \in X_i$, since X_i is finite, we will have a finite cover of X_i. So each X_i is a compact, totally disconnected space. By Proposition 3.1.12, we finally have that $\varprojlim_{i\in I} X_i \cong X$ is also compact and totally disconnected.
(R $\implies$ L) Let X be a compact and totally disconnected space. We wish to show that X is profinite. For this, we would need to construct a projective system of finite discrete spaces $\{X_i\}_{i\in I}$ whose limit would be homeomorphic to X. Let us now divide the rest of the proof in following *acts* for better readability:
Act 1. *Constructing the required projective system.*
Let $\mathfrak{R}$ be the poset of all equivalence relations R on X for which X/R gives a quotient space which is discrete and finite. The arrows in this poset being topological inclusions[24] of one quotient into another. We need to show that $\mathfrak{R}$ is cofiltered, which means that for each $R, S \in \mathfrak{R}$, there is a $T \in \mathfrak{R}$ such that $T \subseteq R$ and $T \subseteq S$ (remember, a poset is cofiltered if each diagram in it has a cone). So let us take any two equivalence relations $R, S \in \mathfrak{R}$. Denote the following to be the (finite) partitions of X induced by R and S, respectively:

$$X = \bigcup_{i=1}^{r} Y_i^R \qquad X = \bigcup_{i=1}^{s} Y_i^S.$$

We can then construct the following partition of X:

$$X = \bigcup_{i=1}^{r}\bigcup_{j=1}^{s} Y_i^R \cap Y_j^S.$$

Clearly, this partition is finite and is contained in both the other partitions. We now need to show whether this partition also induce an equivalence relation which is a member of $\mathfrak{R}$. For this, we just need to show whether this new quotient space has discrete topology. To show that a finite quotient space is discrete, all we have to show is whether each of the class is clopen or not in X, since a set in quotient is open if and only if it's inverse under canonical injection from base to quotient is an open in the base space. We see that since Y_i^R and Y_j^S are all clopen, since X/R and X/S are discrete, hence each $Y_i^R \cap Y_j^S$ is clopen in X, proving that this new partition induces an equivalence relation which is a member of $\mathfrak{R}$ and is contained in each of R and S. Hence $\mathfrak{R}$ is cofiltered.
Act 2. *Constructing a homeomorphism $X \longrightarrow \varprojlim_{R\in\mathfrak{R}} X/R$.*
Our next goal is to look at the limit of the projective system $\mathfrak{R}$. Remember that we wish to find a homeomorphism $X \longrightarrow \varprojlim_{R\in\mathfrak{R}} X/R$. Our candidate for this map would be the canonical quotient map (note that the limiting space is a subspace of product, as given in Lemma 3.1.6):

$$\begin{aligned} \lambda : X &\longrightarrow \varprojlim_{R\in\mathfrak{R}} X/R \\ x &\longmapsto ([x]_R)_{R\in\mathfrak{R}}\,. \end{aligned}$$

Also remember that X is compact & totally disconnected. Moreover, each X/R is finite & discrete, so it is totally connected & compact. Hence by Proposition 3.1.12, $\varprojlim_{R\in\mathfrak{R}} X/R$ is also totally connected &

[24] This means that a quotient $X/Q \subseteq X/R$ for any $x \in X$, $[x]_Q \in X/R$.

compact (in particular compact & Hausdorff). This means that λ is a map between compact Hausdorff spaces. We know that any continuous bijection between compact Hausdorff spaces is a homeomorphism, so we just need to show that λ is a bijection as it is already continuous (λ is the quotient embedding map). Also remember that a continuous map between compact spaces takes a compact subspace to compact subspace, so $\lambda(X) \subseteq \varprojlim_{R\in\mathfrak{R}} R$ is compact. But since $\varprojlim_{R\in\mathfrak{R}} R$ is also Hausdorff, therefore $\lambda(X)$ is a compact subspace (this follows from the fact that a compact subspace of a Hausdorff space is closed; this can be proved by keeping track of disjoint open subsets guaranteed by T_2). So in order to show that λ is a bijection, we just need to show that λ is injection and $\lambda(X)$ is dense in $\varprojlim_{R\in\mathfrak{R}} R$. This is exactly what we will do now.

Act 3. *λ is injective.*

We now show that λ is injective. We will do this by showing that $x \neq y \implies \lambda(x) \neq \lambda(y)$. Now, if $x \neq y$ in X, since X is totally connected and compact, we get that $\exists$ clopen sets $U \ni x$ and $V \ni y$ such that $U \cap V = \emptyset$. We now have the quotient space X/U made by the equivalence relation that $x \sim y \iff x, y \in U$. Clearly X/U is a two point discrete space and so the corresponding relation $\sim$ is in $\mathfrak{R}$. Now, since $([x]_R)_{R\in\mathfrak{R}} \in \varprojlim_{R\in\mathfrak{R}} R$, therefore $[x]_\sim \in X/U$. Remember that $x \in U$, so $[x]_\sim$ represents set of those points of X which are in U. Similarly, since $([y]_R)_{R\in\mathfrak{R}} \in \varprojlim_{R\in\mathfrak{R}} R$, we have that $[y]_\sim \in X/U$, and since $y \notin U$, therefore $[y]_\sim \neq [x]_\sim$. Hence $([x]_R)_{R\in\mathfrak{R}} \neq ([y]_R)_{R\in\mathfrak{R}}$, proving that λ is injective.

Act 4. *$\lambda(X) \subseteq \varprojlim_{R\in\mathfrak{R}} X/R$ is dense.*

We will show this by classical technique of proving that each neighborhood of each point in $\varprojlim_{R\in\mathfrak{R}} X/R$ intersects $\lambda(X)$. So take any point $([x_R]_R)_{R\in\mathfrak{R}} \in \varprojlim_{R\in\mathfrak{R}} X/R$, where $x_R \in X$ is some point chosen from X and $[x_R]_R \in X/R$ is the class corresponding to x_R in the quotient, for each $R \in \mathfrak{R}$. Take any basic open neighborhood of $([x_R]_R)_{R\in\mathfrak{R}} \in \varprojlim_{R\in\mathfrak{R}} X/R \subseteq \prod_{R\in\mathfrak{R}} X/R$, namely, $\prod_{R\in\mathfrak{R}} U_R \cap \varprojlim_{R\in\mathfrak{R}} X/R$ which contains $([x_R]_R)_{R\in\mathfrak{R}}$. Since $\prod_{R\in\mathfrak{R}} X/R$ has product topology, so there exists a finite subset $\mathfrak{F} \subset \mathfrak{R}$ such that $U_R \subset X/R \ \forall R \in \mathfrak{F}$ and $U_R = X/R \ \forall R \notin \mathfrak{F}$. We then note that $[x_R]R \in U_R \subset X/R \ \forall R \in \mathfrak{F}$. We will now find a $x \in X$ such that $\lambda(x)$ would be contained in $\prod_{R\in\mathfrak{R}} U_R \cap \varprojlim_{R\in\mathfrak{R}} X/R$. For this, we first instantiate the following canonical quotient embedding for each $R \in \mathfrak{R}$:

$$\begin{aligned} \pi_R : X &\longrightarrow X/R \\ x &\longmapsto [x]_R. \end{aligned}$$

With this, we then see that the following subset

$$\bigcap_{R\in\mathfrak{F}} \pi_R^{-1}(U_R) \subseteq X$$

is non-empty, open subspace of X. The non-empty part comes from the observation that if this were to be empty, then we would be challenging the projectivity of projective system $\mathfrak{R}$; since $\mathfrak{R}$ is projective and $\mathfrak{F} \subset \mathfrak{R}$, hence there exists $R \in \mathfrak{R}$ such that $R \subseteq R_i$ for all $R_i \in \mathfrak{F}$. Hence, the only way the above intersection can be null if for each of the given $U_{R_i} \subseteq X/R_i$ for $R_i \in \mathfrak{F}$ that we have, we must also have $X/R \cap U_{R_i} = \emptyset$. This is because if we don't have this, then there would be elements common to all $\pi_{R_i}(U_{R_i})^{-1}$, which would contradict the assumption. But now if $X/R \cap U_{R_i} = \emptyset$, then $\pi_{R_i}^{-1}(U_{R_i}) \cap \pi_{R_i}^{-1}(X/R) = \emptyset$ and so $\pi_{R_i}^{-1}(U_{R_i}) \cap X = \emptyset$, i.e. $\pi_{R_i}^{-1}(U_{R_i}) = \emptyset$, which is clearly not possible, hence a contradiction to the assumption that $\bigcap_{R\in\mathfrak{F}} \pi_R^{-1}(U_R) = \emptyset$. The next thing to justify is the claim that this intersection is open. This is easy because each U_{R_i} is open in X/R_i, π_{R_i} is continuous and $\mathfrak{F}$ is finite.

So we have established that $\bigcap_{R\in\mathfrak{F}} \pi_R^{-1}(U_R) \subseteq X$ is non-empty. Now simply take any $x \in \bigcap_{R\in\mathfrak{F}} \pi_R^{-1}(U_R)$. We then note that $\lambda(x) = ([x]_R)_{R\in\mathfrak{R}}$ is such that $[x]_R \in U_R$ for all $R \in \mathfrak{F}$ because of the choice of $([x]_R)_{R\in\mathfrak{R}}$. What we now have is that $\lambda(X) \cap \prod_{R\in\mathfrak{R}} U_R \cap \varprojlim_{R\in\mathfrak{R}} R \neq \emptyset$. Since $\prod_{R\in\mathfrak{R}} U_R \cap \varprojlim_{R\in\mathfrak{R}} R$ was an arbitrary basic open set of $\varprojlim_{R\in\mathfrak{R}} R$, we hence have that the closure of $\lambda(X)$ is whole of $\varprojlim_{R\in\mathfrak{R}} R$, completing the proof. ∎

There are more results on profinite spaces, like the fact that a profinite space has a basis of clopen sets, etc. But we now move on and will cite such results whenever necessary. We now study infinitary Grothendieck's Galois theory.

3.2 Infinitary Grothendieck's Galois theory

With the notion of profinite spaces firm in place, we are now ready to look how the Grothendieck's Galois theorem (Theorem 7) generalizes to infinite dimensional algebras and scalar extensions.

> ***Main goal of this section :*** To establish infinitary Grothendieck's Galois theorem, Theorem 9.

3.2.1 Topological groups

We now set up the important definitions introducing topological groups.

> ***Main goal of this subsection :*** To introduce the definitions of toplogical groups G and G-spaces.

Let us first begin with the classical notion of a topological group:

Definition 3.2.1. (**Topological Group**) *Suppose $(G, \cdot)$ is a group. If G is also equipped with the topology τ on it so that the following two maps are continuous*

$$\begin{aligned} - \cdot - : G \times G &\longrightarrow G \\ (g, h) &\longmapsto g \cdot h \\ (-)^{-1} : G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned}$$

where $G \times G$ has the product topology.

Remark 3.2.2. Let us now explain what the continuity conditions of a topological group actually entails. By Definition 3.2.1, G is a topological group if for each open set $H \subseteq G$, the set $H_1 \times H_2 \subseteq G \times G$ such that $H_1 \cdot H_2 = H$, is open in $G \times G$. As for the second continuity condition, we have that for any open $H \subseteq G$, the set $H^{-1} \subseteq G$ where $H^{-1} = \{h^{-1} \in G \mid h \in H\}$ is open in G.

We now define a topological G-space, which is a generalization of group actions to topological group actions on a topological space:

Definition 3.2.3. (**Topological G-Space**) *Let G be a topological group and X be a topological space. X is said to be a topological G-space if there exists a continuous group action of G on X, that is, the group action:*

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longrightarrow g \star x \end{aligned}$$

is a continuous map from the product space $G \times X$ to space X.

Definition 3.2.4. (**Topological G-space Morphism**) *Consider a topological group G and G-spaces X and Y. A continuous map $f : X \longrightarrow Y$ would be a G-space morphism if f would also be a G-morphism, that is, for any $g \in G$ and $x \in X$, f must follow*

$$f(g \star x) = g \star f(x).$$

We then define a profinite topological G-space:

Definition 3.2.5. (**Profinite Topological G-Space**) *Let G be a topological group. Suppose $\{X_i\}_{i\in I}$ is a projective system of finite, discrete topological G-spaces. The limiting space, $\varprojlim_{i\in I} X_i$ of this system would be defined as a profinite topological G-space.*

We then have the category of profinite G-spaces

Remark 3.2.6. (**Category of Profinite Topological G-Spaces and Morphisms**) Let G be a topological group. The category of all profinite topological G-spaces and G-space morphisms between them is denoted as:

$$G - \textbf{Prof}.$$

Clearly, $G - \textbf{Prof}$ is a subcategory of **Top**.

We now look at the following lemma, which characterizes the requirement for a discrete *G-set* X to be a *G-space*:

Lemma 3.2.7. Let G be a topological group and X be a G-set. Let X have discrete topology. X is a G-space if and only if the stabilizer G_x of G's action on X is open in G for each $x \in X$.

Proof. (L $\implies$ R) Let X be a G-space and choose any $x \in X$. The stabilizer G_x is the following subgroup of G:

$$G_x := \{g \in G \mid g \star x = x\}.$$

We wish to show that G_x is open in G. Since X is a G-space, therefore the group action $G \times X \longrightarrow X$ is a continuous map. Now, X is discrete, therefore $\{x\}$ is open in X, hence the inverse image of the action $\{(g, x) \in G \times X \mid;\ g \star x = x\} = \{g \in G \mid g \cdot x = x\} \times \{x\} \subseteq G \times X$ is open in product topology, which means that $\{g \in G \mid g \cdot x = x\}$ is open in G.
(R $\implies$ L) Let X be a discrete space which is also a G-set. Moreover, let each stabilizer, G_x, for each point $x \in X$ be an open subset of G. We wish to show that X is a G-space, or in other words, the G-action $G \times X \longrightarrow X$ is a continuous map. For this, take any subset $U \subseteq X$ (which is open as X is discrete). Note that $U = \bigcup_{x\in U}\{x\}$. The inverse image under G-action is the following subset of $G \times X$:

$$\bigcup_{x\in U}\{(g, x) \in G \times X \mid g \star x = x\} = \bigcup_{x\in U} G_x \times \{x\}$$

which is open in $G \times X$ as G_x is given open in G and $\{x\}$ is anyways open in X. ■

3.2.2 The profinite **Gal** $[L : K]$-space, $\textbf{Hom}_{\textbf{K-Alg}}(A, L)$.

As the title suggests, we will now see how under appropriate hypotheses, for a K-algebra A, we can treat $\text{Hom}_{\textbf{K-Alg}}(A, L)$ as a **Gal** $[L : K]$-space.

> ***Main goal of this subsection :*** To establish various results surronding $\text{Hom}_{\textbf{K-Alg}}(A, L)$ as a topological **Gal** $[L : K]$-space.

Let us first state with a *sketchy* proof the following result, which says that a Galois group is the limit of the diagram consisting of Galois groups of all finite dimensional intermediary Galois extensions:

Proposition 3.2.8. Let $[L : K]$ be a Galois extension. Denote $\mathfrak{I}_{\text{Fin}}$ to be the poset consisting of all finite dimensional intermediate extensions M as in $[L : M : K]$ and inclusions therein. Then,

$$\textbf{Gal}\,[L : K] \cong \varprojlim_{M \in \mathfrak{I}_{\text{Fin}}} \textbf{Gal}\,[M : K]$$

in **Grp** where for $M \subseteq N$ is mapped to $\textbf{Gal}\,[N : K] \longrightarrow \textbf{Gal}\,[M : K]$, $f \longmapsto f|_M$.

Proof. We wish to prove that the Galois group $\textbf{Gal}\,[L : K]$ has a limiting cone over the diagram $\{\textbf{Gal}\,[M : K]\}_{M \in \mathfrak{I}_{\text{Fin}}}$ For this, consider the cone given by $\alpha_M : \textbf{Gal}\,[L : K] \longrightarrow \textbf{Gal}\,[M : K]$, $(f : L \to L) \longmapsto (f|_M : M \to M)$, where we have to show that $f|_M$ indeed become a K-algebra automorphism $M \to M$. Seeing this latter is easy by taking any such $f : L \to L$ and then taking any $m \in M$, arguing about the minimal polynomial $p(x) \in K[x]$ of m and noticing that $f(m)$ is also a root of $p(x)$, but $[M : K]$ is Galois, so $f(m)$ (a root of $p(x)$) must be in M. All that needs to be shown now that this is indeed universal. In particular, we need to show that a collection of maps $\beta_M : G \longrightarrow \textbf{Gal}\,[M : K]$ for each $M \in \mathfrak{I}_{\text{Fin}}$ such that for any $N \subseteq M$ we have that β_M factors via $\alpha_M : \textbf{Gal}\,[L : K] \longrightarrow \textbf{Gal}\,[M : K]$. This result comes directly from the Proposition 3.1.4, [BJ01]. ∎

We now define a topology on a Galois group, which would make $\text{Hom}_{\textbf{K-Alg}}(A, L)$ a $\textbf{Gal}\,[L : K]$-space:

Definition 3.2.9. (**Topological Galois Group**) *Let $[L : K]$ be a Galois field extension. We say that $\textbf{\textit{Gal}}\,[L : K]$ is a topological Galois group if $\textbf{\textit{Gal}}\,[L : K]$ is given the initial topology with respect to the maps:*

$$p_M : \textbf{\textit{Gal}}\,[L : K] \cong \varprojlim_{M \in \mathfrak{I}_{Fin}} \textbf{\textit{Gal}}\,[M : K] \longrightarrow \textbf{\textit{Gal}}\,[M : K]$$
$$f \longmapsto f|_M$$

where $\mathfrak{I}_{Fin}$ is the poset of finite dimensional intermediate Galois extensions of $[L : K]$ and each $\textbf{\textit{Gal}}\,[M : K]$ is given the discrete topology. The maps p_M are well-defined as shown in Proposition 3.2.8.

Remark 3.2.10. In other words, we are considering the limiting space of the system $\{\textbf{Gal}\,[M : K]_{M \in \mathfrak{I}_{\text{Fin}}}\}$ in the category **Top** where each $\textbf{Gal}\,[M : K]$ is given discrete topology. We know that in **Top** the limiting space is given the initial topology of the limiting cone.
Moreover, the initial topology on $\textbf{Gal}\,[L : K]$ means that this topology has the subbase given by the collection $\{p_M^{-1}(H_M) \mid H_M \subseteq M\}_{M \in \mathfrak{I}_{\text{Fin}}}$. Therefore, the basis of topology on $\textbf{Gal}\,[L : K]$ is the one given by all finite intersections of the form $\bigcap_{i=1,2,\ldots,n} p_{M_i}^{-1}(H_{M_i})$ for any $H_{M_i} \subseteq M_i$ for any finite collection of M_is from $\mathfrak{I}_{\text{Fin}}$. In words, this means that the base of topology on $\textbf{Gal}\,[L : K]$ consists of those subsets $H \subseteq \textbf{Gal}\,[L : K]$ whose elements when restricted to some finitely many finite dimensional Galois subextensions of $[L : K]$ still gives a K-automorphism there.

We now revert our attention back to K-algebras, starting with the fact that an algebraic K-algebras is a filtered union of it's subalgebras, which is a slight generalization of the fact that a finite-dimensional K-algebra is also generated by finitely many of it's subalgebras, as observed in Act 5, Proof of Theorem 6:

Proposition 3.2.11. Let K be a field and A be an algebraic K-algebra. A is then the filtered union of it's finite dimensional algebras.

Proof. Since A is an algebraic K-algebra, therefore any $a \in A$ is an algebraic element. Now, $K(a)$ for some $a \in A$ is a finite dimensional subalgebra of A. The fact that this would be finite dimensional follows from Proposition 2.2.6 (where note the finiteness of $\deg f_a(x)$). In fact any finite dimensional subalgebra of A, say B, is of the form $B = K(a_1, \ldots, a_n)$ for finitely many $a_1, \ldots, a_n \in A$. We therefore have that $A = \bigcup_S S$ where S is a finite dimensional subalgebra of A. We now wish to show that $\{S\}_{S \subseteq A \text{ is fin. dim.}}$

forms a filtered set. To do this, we have to show that for any two finite dimensional subalgebras $B, C \subseteq A$, there is a subalgebra $D \subseteq A$ such that $D \supseteq B$ and $D \supseteq C$. As we noted earlier, B and C is of the form:

$$B = K(b_1, \ldots, b_n)\ ,\ \ C = K(c_1, \ldots, c_m)$$

where $b_i, c_j \in A$ and n, m are finite. Now, to construct this bigger subalgebra subsuming these two, we simply look at the following subalgebra,

$$D := K(b_1, \ldots, b_n, c_1, \ldots, c_m).$$

Clearly D contains B and C. It remains to be shown that D is also finite dimensional. For this, we remind ourselves that $K(b_1, \ldots, b_n, c_1, \ldots, c_m) = \{p(b_1, \ldots, b_n, c_1, \ldots, c_m) \in A \mid p(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}) \in K[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}]\}$. Now suppose D as above is infinite dimensional. Note that in an infinite dimensional algebra, one cannot write each element as a linear combination of a bounded amount of fixed elements as the algebra doesn't remains infinite dimensional. Then there is no collection of finitely many independent elements of A which spans whole of A. But remember that each $b_i, c_j \in A$ have minimal polynomials $f_{b_i}, f_{c_j} \in K[x]$ such that $f_{b_i}(b_i) = f_{c_j}(c_j) = 0$. This means that all finite powers of b_i are linear combinations of only b_i^k where $0 \leq k < \deg f_{b_i}$. Similarly for c_j. This gives us that any element D can be given by resultant of application on all polynomials in $n + m$ variable of degree atmost $N = \max_{1 \leq i \leq n, 1 \leq j \leq m}\{\deg f_{b_i}, \deg f_{c_j}\} - 2$ of $b_1, \ldots, b_n, c_1, \ldots, c_m$. We thus have that each element of D can be given by linear combination of fixed elements of D, the total number of which is bounded. But that cannot happen if D is infinite dimensional. Therefore D is finite dimensional. Hence proved. ■

We will now use the result just proved, Proposition 3.2.11, quite frequently[25]. We next use this result to show that $\mathrm{Hom}_{\textbf{K-Alg}}(A, L)$ is a profinite space for any (arbitrary dimensional) Galois extension $[L : K]$ for a K-algebra A which is split by L:

Proposition 3.2.12. Let $[L : K]$ be an arbitrary dimensional Galois extension of field K. If A is an algebraic K-algebra which is split by L, then there exists the following bijection:

$$\mathrm{Hom}_{\textbf{K-Alg}}(A, L) \cong \varprojlim_{S \in \mathfrak{A}} \mathrm{Hom}_{\textbf{K-Alg}}(S, L)$$

where $\mathfrak{A}$ is the filtered poset of all finite dimensional subalgebras of A and $\mathrm{Hom}_{\textbf{K-Alg}}(S, L)$ is **finite** for each $S \in \mathfrak{A}$.

Proof. Let us first prove the bijection. By Proposition 3.2.11, we have that $A = \bigcup_{S \in \mathfrak{A}} S$ where $\mathfrak{A}$ is filtered. We therefore have that $\{\mathrm{Hom}_{\textbf{K-Alg}}(S, L)\}_{S \in \mathfrak{A}}$ is cofiltered. This yields us that $\mathrm{Hom}_{\textbf{K-Alg}}(A, L) = \mathrm{Hom}_{\textbf{K-Alg}}\left(\bigcup_{S \in \mathfrak{A}}, L\right) = \mathrm{Hom}_{\textbf{K-Alg}}\left(\varinjlim_{S \in \mathfrak{A}} S, L\right) \cong \varprojlim_{S \in \mathfrak{A}} \mathrm{Hom}_{\textbf{K-Alg}}(S, L)$ where the last isomorphism follows from the fact that if we take any cone over $\{\mathrm{Hom}_{\textbf{K-Alg}}(S, L)\}_{S \in \mathfrak{A}}$, we equivalently have a cocone over $\mathfrak{A}$, and therefore each component of the cone factors via the $\mathrm{Hom}_{\textbf{K-Alg}}\left(\varinjlim_{S \in \mathfrak{A}} S, L\right)$.
We next wish to show that $\mathrm{Hom}_{\textbf{K-Alg}}(S, L)$ for any $S \in \mathfrak{A}$ is a finite algebra. To show this, we wish to use the Theorem 6, 5. For that, we first note that S is already a finite dimensional K-algebra, but $[L : K]$ may not be finite dimensional. But to remedy this, we use the unproved fact that any for any finite dimensional K-algebra S split by a Galois extension $[L : K]$, there exists a finite dimensional intermediate Galois extension $[L : M : K]$ where M also splits S. Therefore, $\mathrm{Hom}_{\textbf{K-Alg}}(S, M)$ would be finite by Theorem 6, 5. We just need to show that $\mathrm{Hom}_{\textbf{K-Alg}}(S, L)$ is either isomorphic to $\mathrm{Hom}_{\textbf{K-Alg}}(S, M)$ or to some of it's subset. To see this, take any $s \in S$ and any $f \in \mathrm{Hom}_{\textbf{K-Alg}}(S, L)$. We will now show that $f(s) \in M$. For this, first denote the minimal polynomial $p_s(x) \in K[x]$ of $s \in S$, and then note that since f is a K-algebra

[25]This is something that you might have expected as the nature of this result suggests that one can construct a filtered system of finite dimensional subalgebras of any given (algebraic) algebra, and so one can now talk about what the limit of this system may look like, in hope of connecting back to profinite spaces.

homomorphism, therefore we must have that $0 = f(0) = f(p_s(s)) = p_s(f(s))$, therefore $f(s)$ is also a root of $p_s(x)$. But $[M : K]$ splits S, therefore each root of $p_s(s)$ must lie in M and in particular, $f(s)$ must lie in M. Therefore each member of $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)$ is a member of $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, M)$, where the latter is finite, and hence so is the former, completing the proof. ■

It is clear from the above that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$ is a profinite space:

Corollary 3.2.13. Let $[L : K]$ be an arbitrary dimensional Galois extension of field K. If A is an algebraic K-algebra which is split by L, then $\mathrm{Hom}_{\mathbf{K\text{-}alg}}(A, L)$ is a profinite space.

Proof. Under the same hypotheses as of Proposition 3.2.12, we have proved that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) \cong \varprojlim_{S \in \mathfrak{A}} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, K)$ where $\mathfrak{A}$ is the filtered poset of all finite dimensional subalgebras of A. Clearly, if $\{S\}_{S \in \mathfrak{A}}$ is filtered, then $\{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)\}_{S \in \mathfrak{A}}$ is cofiltered. Hence if we regard each $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)$ as a discrete space and hence as a member of **Top**, then we see that the projective system $\{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)\}_{S \in \mathfrak{A}}$ in **Top** has a limiting space given by $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$. This proves the result. ■

We now come to an important step in understanding the action of Galois group $\mathbf{Gal}\,[L : K]$ on the space $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$, the latter now already known to be a profinite space (Corollary 3.2.13):

Proposition 3.2.14. Let $[L : K]$ be an arbitrary Galois extension of the field K and A be any K-algebra which is split by L. Give the group $\mathbf{Gal}\,[L : K]$ the topology as in Definition 3.2.9 and the set $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$ the topology as inherited from being a profinite space[26]. The map

$$\begin{aligned} \mu : \mathbf{Gal}\,[L : K] \times \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) &\longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) \\ (g, f) &\longmapsto g \circ f \end{aligned}$$

then defines a continuous action of the topological Galois group $\mathbf{Gal}\,[L : K]$ on the space $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$. This makes the space $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$ a topological $\mathbf{Gal}\,[L : K]$-space.

Proof. We wish to show that μ as defined is a) continuous, b) satisfies $g_1 \circ (g_2 \circ f) = (g_1 \circ g_2) \circ f$. The b) is trivial. We are left with the task of showing a), that μ is continuous. Remember that to establish continuity of a map to a space which is given the initial topology, it is enough to establish continuity of it's pre-composition with each member. This is what we will do now; for each $S \in \mathfrak{A}$ denote the projection $q_S : \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) \longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)$ and similarly for each $M \in \mathfrak{I}_{\mathrm{Fin}}$, denote the projection $p_M : \mathbf{Gal}\,[L : K] \longrightarrow \mathbf{Gal}\,[M : K]$. As discussed earlier, we wish to show that for any $S \in \mathfrak{A}$ the composition $q_S \circ \mu : \mathbf{Gal}\,[L : K] \times \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) \longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)$ is continuous. We will now show that $q_S \circ \mu$ is equal to certain other composition, where each member would be continuous, which would hence complete the proof. First remember that since $S \subset A$ is finite dimensional and L splits A, therefore there exists a finite dimensional Galois subextension $[L : M : K]$ which splits S. Now consider the following diagram:

$$\mathbf{Gal}\,[L : K] \times \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) \xrightarrow{p_M \times 1} \mathbf{Gal}\,[M : K] \times \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) \xrightarrow{1 \times q_S} \mathbf{Gal}\,[M : K] \times \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L) \xrightarrow{(g,f) \mapsto g \circ f}$$

where the last map is well-defined because $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L) \cong \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, M)$ using the same argument which utilizes that any map $f : S \to L$ maps values to M because M splits S. Hence last map $(g, f) \mapsto g \circ f$ is an isomorphism. Since p_M and q_S are continuous, therefore so is their composite, hence the above diagram is continuous. Finally, for any $(g, f) \in \mathbf{Gal}\,[L : K] \times \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$, the above composite takes it to $(g, f) \mapsto (g|_M, f) \mapsto (g|_M, f|_S) \mapsto g|_M \circ f|_S = g \circ f|_S = q_S(\mu(g, f))$. Hence proved. ■

[26] That is, it has initial topology as obtained by the components of the limiting cone over $\{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)\}_{S \in \mathfrak{A}}$, as in Proposition 3.2.12.

Comments on Proof Technique. One of the techniques that we should now keep in mind in proving if a map is continuous in **Top** is that whether it can be written as a composite of some continuous maps. Even though it sounds obvious, but as shown in the above proof, it can be a bit elusive. The other way to show that $q_S \circ \mu$ is continuous would've been the usual method of taking a sub-basic open set in $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$ and finding an inverse under $q_S \circ \mu$, which is evidently a bit more difficult as compared to the method employed above.

We have established in Proposition 3.2.14 that a K-algebra A which is split by a Galois extension L gives a profinite K-algebra $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$ which moreover has a continuous action of topological Galois group $\mathbf{Gal}\,[L : K]$. It is now natural to ask if a K-algebra homomorphism between two such algebras also induces a topological $\mathbf{Gal}\,[L : K]$ map. We answer in the affirmative, as shown by the following result:

Proposition 3.2.15. Let $[L : K]$ be an arbitrary dimensional Galois extension of field K and A, B be two K-algebras split by L with a K-algebra homomorphism $f : A \longrightarrow B$. Then the map

$$\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L) : \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L) \longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$$

is a topological $\mathbf{Gal}\,[L : K]$ morphism where $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L), \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L)$ has the profinite topology as shown in Corollary 3.2.13 and $\mathbf{Gal}\,[L : K]$ is the topological Galois group.

Proof. To prove this, we first show that for any $g \in \mathbf{Gal}\,[L : K]$ and for any $h \in \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L)$, we have $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L)(g \circ h) = g \circ \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L)(h)$. This is quite easy as $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L)(g \circ h) = g \circ h \circ f = g \circ \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L)(h)$. Next, we need to show that the map $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L)$ is a continuous map. For this take any finite dimensional subalgebra of A, $S \in \mathfrak{A}$ and remember from Proposition 3.2.12 that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) \cong \varprojlim_{S \in \mathfrak{A}} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)$. Denote the corresponding projection as $p_S : \mathrm{Hom}_{\mathbf{K}}(A, L) \longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)$. Now, since $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$ has initial topology of all these projection p_S, therefore to show the continuity of map $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L)$, it is enough to show continuity of $p_S \circ \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L) : \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L) \longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L)$. This is what we will establish now. As usual, we will prove that this composite is equal to some other composite of already continuous maps. In particular, note that $f(S) \subset B$ is also a finite dimensional subspace of B as for any $b \in f(S)$ and $s_1, \ldots, s_n \in S \subset A$ the finite basis of S, we can write $b = \sum_{i=1}^{n} f(k_i s_i) = \sum_{i=1}^{n} k_i f(s_i)$. Thus, $f(S) \in \mathfrak{B}$. By Proposition 3.2.12, we have that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L) \cong \varprojlim_{T \in \mathfrak{B}} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(T, L)$, in particular, we have the continuous projection $q_{f(S)} : \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L) \longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f(S), L)$, $h \longmapsto h|_{f(S)}$. Now, let us look at the composite

$$\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L) \xrightarrow{q_{f(S)}} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f(S), L) \xrightarrow{-\circ f|_S} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S, L).$$

For any $h \in \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L)$, we have the following mapping from the above composite $h \mapsto h|_{f(S)} \mapsto h|_{f(S)} \circ f|_S = (h \circ f)|_S = p_S \circ \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L)(h)$. Hence the above composite is equal to $p_S \circ \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(f, L)$ and since each member in the above composite is continuous ($- \circ f|_S$ is continuous as it is a map between finite discrete spaces), we hence have our result. ∎

Remark 3.2.16. (**Dé jà Vu**) Propositions 3.2.14 and 3.2.15 together shows that for a topological Galois group $\mathbf{Gal}\,[L : K]$ and a K-algebra A which is split by extension L, we have that the K-algebra $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L)$ with it's profinite topology given by the poset of finite-dimensional subalgebras of A is a $\mathbf{Gal}\,[L : K]$-space and moreover, each morphism of such K-algebras split by L gives a map of $\mathbf{Gal}\,[L : K]$-spaces. What this suggests us is that the functor $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(-, L) : \mathbf{K\text{-}Alg}^{\mathrm{op}} \longrightarrow \mathbf{Sets}$ restricts to $\mathbf{Split}_K(L)$ to give the following functor, just like in Theorem 7, but this time, there's no $_{\mathrm{Fin}}$:

$$\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(-, L) : \mathbf{Split}_K(L) \longrightarrow \mathbf{Gal}\,[L : K] - \mathbf{Prof}$$

where $\mathbf{Split}_K(L)$ is the full-subcategory of $\mathbf{K\text{-}Alg}$ of all those K-algebras which are split by L. Indeed, we will soon see that this functor establishes an equivalence of categories, and this would be our fundamental theorem of infinitary Grothendieck's Galois theory.

Then next is a minor result needed only for a small part in our proof of the fundamental theorem:

Lemma 3.2.17. Let A be an algebraic K-algebra and B be any finite dimensional K-algebra. Consider the filtered poset $\mathfrak{A}$ of all finite dimensional subalgebras of A, and this gives a filtered system of sets $\left\{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,S)\right\}_{S\in\mathfrak{A}}$. Moreover, we have a cocone over this system given by maps

$$\begin{aligned} i_S : \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,S) &\longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,A) \\ (B\to S) &\longmapsto (B\to S\hookrightarrow A) \end{aligned}$$

for each $S\in\mathfrak{A}$. Then, the universal map

$$\rho : \varinjlim_{S\in\mathfrak{A}} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,S) \longrightarrow \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,A)$$

is an isomorphism in **Sets**.

Proof. Let us first prove the injectivity of ρ. For this, take $g,h\in\varinjlim_{S\in\mathfrak{A}}\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,S)$. Clearly, for some $S_g,S_h\in\mathfrak{A}$, we will have that $g\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,S_g)$ and $h\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,S_h)$. By filteredness of the system, we can assume that there exists $S\in\mathfrak{A}$ such that $g,h\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,S)$. Now, let $\rho(g)=\rho(h)\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,A)$, where they are given by $\rho(g)=i_S(g)$ and $\rho(h)=i_S(h)$, then clearly $g=h$. To see surjectivity, take any $f\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,A)$. Since B is finite dimensional, therefore let $\{b_i\}_{i=1}^n$ be a basis of B. Since $A=\varinjlim_{S\in\mathfrak{A}}=\bigcup_{S\in\mathfrak{A}}S$, therefore $f(b_i)\in S_i$ for some $S_i\in\mathfrak{A}$ for each $i=1,\ldots,n$. Again, by filteredness of $\mathfrak{A}$ (Proposition 3.2.11), we will have an $S\in\mathfrak{A}$ such that $f(b_i)\in S\ \forall i=1,\ldots,n$. We then have that $f\in\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,S)$ since $\{b_i\}$ is the basis of B and each $f(b_i)\in S$. Now, $f=i_S(f)=\rho(\bar{f})$ for some $\bar{f}$ in the colimit because ρ is the universal map, and therefore we must have that ρ is surjective. Hence proved. ∎

Remark 3.2.18. Lemma 3.2.17 shows that the colimit of the filtered system $\left\{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,S)\right\}_{S\in\mathfrak{A}}$ is indeed the one that we would expect it to be, $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,A)$.

Next we see that a profinite group G, that is a group which is a projective limit of finite discrete topological groups, gives us a *covering*[27] of the category $G-\mathbf{Top}_{\mathrm{Fin}}$ of all discrete finite topological G-spaces and G-space morphisms:

Lemma 3.2.19. Let $G=\varprojlim_{i\in I}G_i$ be a profinite group where G_i is a discrete finite topological group and I is (obviously) a cofiltered index set. For each $i\in I$, we have a category $G_i-\mathbf{Sets}_{\mathrm{Fin}}$ of finite G_i-sets and G_i-morphisms[28] and the category $G-\mathbf{Top}_{\mathrm{Fin}}^{\mathrm{Dscrt}}$ of discrete finite G-spaces and G-space morphisms. If each $p_i:G\longrightarrow G_i$ is a surjective homomorphism, then for each $i\in I$, there exists the functor

$$\begin{aligned} \gamma_i : G_i-\mathbf{Sets}_{\mathrm{Fin}} &\longrightarrow G-\mathbf{Top}_{\mathrm{Fin}}^{\mathrm{Dscrt}} \\ (X,(g_i,x)\mapsto g_i\star x) &\longmapsto (X,(g,x)\mapsto p_i(g)\star x) \end{aligned}$$

which determines $G_i-\mathbf{Sets}_{\mathrm{Fin}}$ as a full-subcategory of $G-\mathbf{Top}_{\mathrm{Fin}}^{\mathrm{Dscrt}}$ which additionally satisfies that

$$\begin{aligned} G-\mathbf{Top}_{\mathrm{Fin}}^{\mathrm{Dscrt}} &\cong \coprod_{i\in I} G_i-\mathbf{Sets}_{\mathrm{Fin}} \\ &\cong \varinjlim_{i\in I}\left(G_i-\mathbf{Sets}_{\mathrm{Fin}}\right) \end{aligned}$$

in the category of all small categories **Cat**.

[27] *covering* in the naive sense, not something concrete like Grothendieck topologies!

[28] Note that we could have also denoted this category as $G_i-\mathbf{Top}_{\mathrm{Fin}}^{\mathrm{Dscrt}}$ of all discrete finite G_i-spaces and G_i-space morphisms because the topology on G_i is discrete and any finite G_i-set, when equipped with discrete topology, becomes an object of $G_i-\mathbf{Top}_{\mathrm{Fin}}^{\mathrm{Dscrt}}$. Similarly, any map $X\to Y$ in $G_i-\mathbf{Sets}_{\mathrm{Fin}}$ is a continuous G_i-map $X\to Y$ when X and Y are given discrete topologies. In short

$$G_i-\mathbf{Sets}_{\mathrm{Fin}}\cong G_i-\mathbf{Top}_{\mathrm{Fin}}^{\mathrm{Dscrt}}.$$

Proof. The existence of functor γ_i is as follows. We first show that γ_i is well-defined. Let $f : X \to Y$ be an arrow in $G_i - \mathbf{Sets}_{\mathrm{Fin}}$. We then have $\gamma_i(f) : \gamma_i(X) \to \gamma_i(Y)$, which we want to show is a continuous G-morphism. This is continuous as $\gamma_i(X) = X$, $\gamma_i(Y) = Y$ and $\gamma_i(f) = f$ but we now consider X, Y as finite discrete spaces, so f, which previously was just a set map, would now be a continuous map. We next want to show that f is a G-space morphism with the new action of G defined on X and Y. For this, take any $g \in G$ and note that $f(p_i(g) \star x) = p_i(g) \star f(x)$ as f is a G_i-map and $p_i(g) \in G_i$. So the functor γ_i is well-defined. Next, we need to establish that γ_i is a full-faithful functor, or, is isomorphism on homsets. Faithful is trivial to see. Fullness is obtained from the fact that for any $f : X \to Y$ in $G - \mathbf{Top}^{\mathrm{Dscrt}}_{\mathrm{Fin}}$ and $g \in G$, we have $f(p_i(g) \star x) = p_i(g) \star f(x)$ and since p_i is surjective, therefore for any $g_i \in G_i$, there is a $g \in G$ such that $g_i = p_i(g)$, and so f is also an arrow in $G_i - \mathbf{Sets}_{\mathrm{Fin}}$ which is mapped to f by γ_i.
Next, we wish to show the latter assertion of the result. For this, first note that any X in $G_i - \mathbf{Sets}_{\mathrm{Fin}}$ is already in $G - \mathbf{Top}^{\mathrm{Dscrt}}_{\mathrm{Fin}}$ as the former is a full-subcategory of the latter. So we just wish to show that any object X of $G - \mathbf{Top}^{\mathrm{Dscrt}}_{\mathrm{Fin}}$ is present in $G_b - \mathbf{Sets}_{\mathrm{Fin}}$ for some $b \in I$. First note that $\varprojlim_{i \in I} G_i \times X \cong \varprojlim_{i \in I}(G_i \times X)$. The action $\varprojlim_{i \in I}(G_i \times X) \cong (\varprojlim_{i \in I} G_i) \times X = G \times X \longrightarrow X$ gives a map $h \in \mathrm{Hom}_{\mathbf{Top}}(G_b \times X, X)$ which allows us to write $\varprojlim_{i \in I}(G_i \times X) \cong G \times X \xrightarrow{p_b \times 1} G_b \times X \xrightarrow{h} X$ to be same as action of G on X above. We just need to show that h is an action of G_b on X. This follows easily from the surjectivity of p_b and the fact the above composite is the action of G onto X; $h(g_b, x) = h(p_b(g), x) = g \star x$ and similarly $h(g_{1b} g_{2b}, x) = h(p_b(g_1) p_b(g_2), x) = h(p_b(g_1 g_2), x) = (g_1 g_2) \star x$. Hence proved. ∎

We finally state the infinitary Grothendieck's Galois theorem:

Theorem 9. (**Fundamental Theorem of Infinitary Grothendieck's Galois Theory**) Let $[L : K]$ be an arbitrary dimensional Galois extension of the field K and let $\mathbf{Gal}[L : K]$ be it's topological Galois group. Denote by $\mathbf{Split}_K(L)$ the category of all K-algebras split by L[29] and by $\mathbf{Gal}[L : K] - \mathbf{Prof}$ the category of all profinite $\mathbf{Gal}[L : K]$-spaces. Then, the functor

$$\mathbf{Split}_K(L) \xrightarrow{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(-, L)} \mathbf{Gal}[L : K] - \mathbf{Prof}$$

establishes an equivalence of categories. That is,

$$\boxed{\mathbf{Split}_K(L) \equiv \mathbf{Gal}[L : K] - \mathbf{Prof}.}$$

Proof. We first prove that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(-, L)$ is full and faithful. For this, let us amalgamate all the things which we have covered so far in this subsection. Take any K-algebras A, B which are split by L (i.e. take any two objects of $\mathbf{Split}_K(L)$). By Proposition 3.2.11, we have that $A = \varinjlim_{S^A \in \mathfrak{A}} = \bigcup_{S^A \in \mathfrak{A}} S^A$ and similarly $B = \varinjlim_{S^B \in \mathfrak{B}} = \bigcup_{S^B \in \mathfrak{B}} S^B$. Furthermore, the Proposition 3.2.12 tells us that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L) = \varprojlim_{S^A \in \mathfrak{A}} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^A, L)$ and similarly $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L) = \varprojlim_{S^B \in \mathfrak{B}} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^B, L)$. Now, we know that there exists an finite dimensional intermediate Galois subextension M^A as in $[L : M^A : K]$ which splits S^A, similarly there exists M^B which splits S^B. Since finite dimensional Galois subextensions forms a filtered poset, therefore there exists a bigger finite dimensional Galois subextension M as in $[L : M : K]$ which contains M^A and M^B and thus splits both S^A and S^B. Finally, we saw multiple times before that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^A, L) \cong \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^A, M^A)$ and similarly for S^B, which we can extend to $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^A, L) \cong \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^A, M)$ and similarly $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^B, L) \cong \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^B, M)$ as M also splits both S^A and S^B. Therefore, we can write

$$\begin{aligned}
\mathrm{Hom}_{\mathbf{Gal}[L:K]-\mathbf{Prof}}\left(\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A, L), \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B, L)\right) &\cong \mathrm{Hom}_{\mathbf{Gal}[L:K]-\mathbf{Prof}}\left(\varprojlim_{S^A \in \mathfrak{A}} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^A, L), \varprojlim_{S^B \in \mathfrak{B}} \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^{} \right. \\
&\cong \varprojlim_{S^B \in \mathfrak{B}} \varinjlim_{S^A \in \mathfrak{A}} \mathrm{Hom}_{\mathbf{Gal}[L:K]-\mathbf{Prof}}\left(\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^A, L), \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^{L}\right. \\
&\cong \varprojlim_{S^B \in \mathfrak{B}} \varinjlim_{S^A \in \mathfrak{A}} \mathrm{Hom}_{\mathbf{Gal}[L:K]-\mathbf{Prof}}\left(\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^A, M), \mathrm{Hom}_{\mathbf{K\text{-}Alg}}(S^{}\right.
\end{aligned}$$

[29] This is a full subcategory of **K-Alg**.

since $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(S^A, M\right)$ and $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(S^B, M\right)$ are finite because of Theorem 6, 5 as S^A, S^B are finite dimensional subalgebras and $[M : K]$ is finite dimensional, therefore the finitary Grothendieck's Galois theorem (Theorem 7) tells us that,

$$\begin{aligned}\varprojlim_{S^B\in\mathfrak{B}}\varinjlim_{S^A\in\mathfrak{A}}\mathrm{Hom}_{\mathbf{Gal}\,[L:K]-\mathbf{Prof}}\left(\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(S^A,M\right),\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(S^B,M\right)\right)&\cong\varprojlim_{S^B\in\mathfrak{B}}\varinjlim_{S^A\in\mathfrak{A}}\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(S^B,S^A\right)\\&\cong\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\varinjlim_{B\in\mathfrak{B}}S^B,\varinjlim_{S^A\in\mathfrak{A}}S^A\right)\\&\cong\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(B,A\right)\end{aligned}$$

which is what we wanted to show.
Now, we wish to see that $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(-,L\right)$ is essentially surjective. For this, take profinite $\mathbf{Gal}\left[L:K\right]$-space X. We wish to find a K-algebra A which is split by L such that

$$\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A,L\right)\cong X.$$

Since X is a profinite $\mathbf{Gal}\left[L:K\right]$-space, therefore there is a projective system $\{X_i\}_{i\in I}$ such that $X\cong\varprojlim_{i\in I}X_i$ where each X_i is a finite discrete $\mathbf{Gal}\left[L:K\right]$-space, i.e. $X_i\in\mathbf{Gal}\left[L:K\right]-\mathbf{Sets}_{\mathrm{Fin}}$. Now since $\mathbf{Gal}\left[L:K\right]$ is a topological Galois group, therefore $\mathbf{Gal}\left[L:K\right]\cong\varprojlim_{j\in J}\mathbf{Gal}\left[M_j:K\right]$ where each M_j is a finite dimensional Galois subextension as in $[L:M_j:K]$. Note that the projection $\mathbf{Gal}\left[L:K\right]\cong\varprojlim_{j\in J}\mathbf{Gal}\left[M_j:K\right]\longrightarrow\mathbf{Gal}\left[M_j:K\right]$, $f\longmapsto f|_{M_j}$ is surjective because each K-automorphism of M_j can be extended to a K automorphism of L by Proposition 1.4.4. We thus infer from Lemma 3.2.19 that $\mathbf{Gal}\left[L:K\right]-\mathbf{Sets}_{\mathrm{Fin}}\cong\coprod_{j\in J}\mathbf{Gal}\left[M_j:K\right]-\mathbf{Sets}_{\mathrm{Fin}}$. Moreover, from the finitary Grothendieck's Galois theorem (Theorem 7), we have that $\mathbf{Gal}\left[M_j:K\right]-\mathbf{Sets}_{\mathrm{Fin}}\equiv\mathbf{Split}_K\left(M_j\right)_{\mathrm{Fin}}$. We therefore have the following

$$\mathbf{Split}_K\left(L\right)_{\mathrm{Fin}}\equiv\mathbf{Gal}\left[L:K\right]-\mathbf{Sets}_{\mathrm{Fin}}\cong\coprod_{j\in J}\mathbf{Gal}\left[M_j:K\right]-\mathbf{Sets}_{\mathrm{Fin}}\equiv\coprod_{j\in J}\mathbf{Split}_K\left(M_j\right)_{\mathrm{Fin}}.$$

Therefore, by Lemma 3.2.19 again, we have that $X_i\in\mathbf{Gal}\left[M_i:K\right]-\mathbf{Sets}_{\mathrm{Fin}}$ for each $i\in I$. Thus, by Theorem 7, we have that $\exists A_i\in\mathbf{Split}_K\left(M_i\right)_{\mathrm{Fin}}$ such that

$$X_i\cong\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A_i,M_i\right)\cong\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A_i,L\right)\,\forall i\in I.$$

Now, we have the following chain,

$$X\cong\varprojlim_{i\in I}X_i\cong\varprojlim_{i\in I}\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A_i,L\right)\cong\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(\varinjlim_{i\in I}A_i,L\right),$$

which reduces our task to finding whether the colimit $\varinjlim_{i\in I}A_i$[30] of K-algebras A_i split by M_i, is split by L. First of all, let us denote $A:=\varinjlim_{i\in I}A_i$ and denote by $\iota_i:A_i\longrightarrow A$ the colimit injection in **K-Alg**. Now, take any $a\in A$. Clearly, there exists $n\in I$ and $b\in A_n$ such that $\iota_n(b)=a$. Remember that A_i is split by M_i, therefore let $p_n(x)\in K[x]$ denote the minimal polynomial of $b\in A_i$, which factors linearly and simply in $M_i[x]$. Finally, note that $p_n(\iota_n(b))=\iota(p_n(b))=0$ which tells us that A is an algebraic K-algebra, and then if we denote $q(x)\in K[x]$ to be the minimal polynomial of $a\in A$, we then get that $q(x)$ must be a factor of $p_n(x)$ as $p_n(a)=0$ but $p_n(x)$ factors linearly and simply in $L[x]$, and hence so does $q(x)$ in $L[x]$. This proves that indeed A is a K-algebra split by L for which $\mathrm{Hom}_{\mathbf{K\text{-}Alg}}\left(A,L\right)\cong X$, and thus completes the proof. ■

[30] computed in **K-Alg**, as visible from above chain.

Interlude

With this, we have concluded the study of Galois theories over fields and commutative algebras in both finitary and infinitary case. We will now study some more *exotic* Galois theories which are more abstract and generalizes all the ones which we have studied so far and also one which we haven't, namely Galois theory for commutative rings; this is categorical Galois theory of Janelidze.
One of the first question that one may face to such an endeavor is the following : *What do one mean by a Galois extension of, say rings in particular and objects of a suitable category in general?*
As we shall see later, this question is answered naturally by what are called *effective descent morphisms*, the study of which requires the knowledge of monads from category theory, which we will next initiate. We will then learn about the categorical Galois theory and will present as one of it's examples the Galois theory of commutative rings and indeed, we will study this latter topic in a lot more detail as compared to what an example demands of itself usually because Galois theory of commutative rings uses quite interesting range of topics, like Pierce spectrum, Stone duality, etc which we would like to study to an appreciable depth.

4 Monads

A *monad* in a category $\mathbf{C}$ is a monoid object in the category of endofunctors of $\mathbf{C}$ with operation being that of composition. The importance of this will become clear to us when we'll see that every adjunction gives rise to a monad and every monad can be defined by a suitable adjunction. We will then see the relation between *algebras* and monads. Here algebra mean the more general one from first order logic; say, the one which may have more than 7 function symbols typical of K-algebras. This will lead us naturally to monadicity of a functor, something that is our prime goal.

Main goal of this section : To introduce monadic functors.

A composition of a functor $F : \mathbf{C} \to \mathbf{C}$ with a natural transformation $\alpha : F \Rightarrow F$ is defined in the obvious way; $F \circ \alpha : F \circ F \Rightarrow F \circ F$ such that for $C \in \mathbf{C}$, $(F \circ \alpha)_C := F(\alpha_C)$, similarly, $(\alpha \circ F)_C := \alpha_{FC}$. Let us now see the formal definition of a monad:

Definition 4.0.1. (**Monad**) *Let $\boldsymbol{C}$ be a category. A monad in $\boldsymbol{C}$ is given by a triple information $(\mathbb{T}, \eta, \mu)$ where*

1. *$\mathbb{T}$ is an endofunctor of $\boldsymbol{C}$:*

$$\mathbb{T} : \boldsymbol{C} \longrightarrow \boldsymbol{C}$$

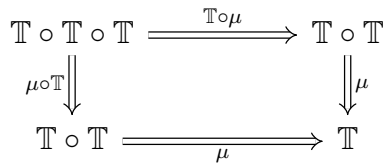
2. *η is a natural transformation from $1_{\mathbf{C}}$ to $\mathbb{T}$, called the **unit of the monad**:*

$$\eta : 1_{\mathbf{C}} \Longrightarrow \mathbb{T}$$

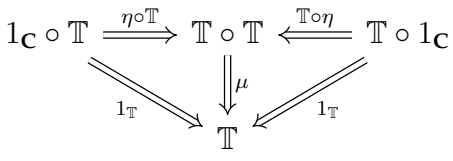
3. *μ is a natural transformation from $\mathbb{T} \circ \mathbb{T}$ to $\mathbb{T}$, called the **multiplication of the monad**:*

$$\mu : \mathbb{T} \circ \mathbb{T} \Longrightarrow \mathbb{T}.$$

and this triple satisfies the following two commutative diagrams:



$\mu\circ(\mu\circ\mathbb{T})=\mu\circ(\mathbb{T}\circ\mu)$
Associativity



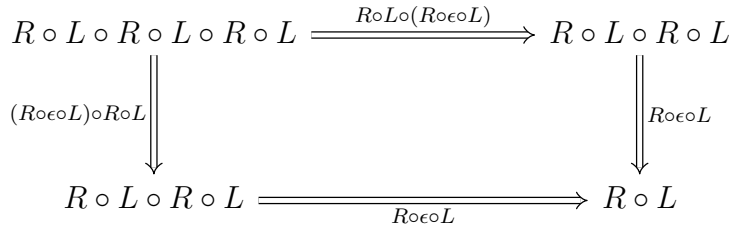
$\mu\circ(\eta\circ\mathbb{T})=\mu\circ(\mathbb{T}\circ\eta)=1_{\mathbb{T}}$
Left/Right Unitality

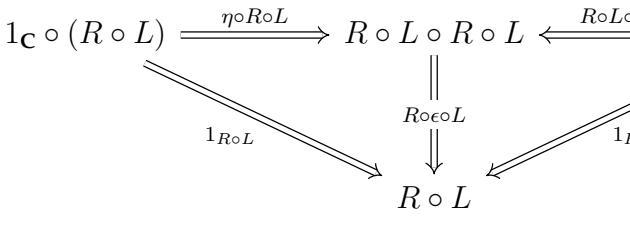
Remark 4.0.2. One can interpret the two commutative diagrams above as follows: if (t, u, v) is some *element* of $\mathbb{T} \circ \mathbb{T} \circ \mathbb{T}$ in the loose sense, then associativity of the monad tells us that $\mu \circ (\mu \circ \mathbb{T})(t, u, v) = (t \cdot u) \cdot v = t \cdot (u \cdot v) = \mu \circ (\mathbb{T} \circ \mu)(t, u, v)$. Similarly, $\mu \circ (\eta \circ \mathbb{T})(t) = 1 \cdot t = t \cdot 1 = \mu \circ (\mathbb{T} \circ \eta)(t) = t = 1_{\mathbb{T}}(t)$.

We now see that each adjunction gives a monad:

Lemma 4.0.3. Let $L : \mathbf{C} \rightleftarrows \mathbf{D} : R$ be an adjunction between categories $\mathbf{C}$ and $\mathbf{D}$ whose unit is $\eta : 1_{\mathbf{C}} \Longrightarrow R \circ L$ and the counit is $\epsilon : L \circ R \Longrightarrow 1_{\mathbf{D}}$. Then, the triple $(R \circ L, \eta, R \circ \epsilon \circ L)$ is a monad on $\mathbf{C}$.

Proof. We have $R \circ L : \mathbf{C} \longrightarrow \mathbf{C}$, $\eta : 1_{\mathbf{C}} \Longrightarrow R \circ L$ and $R \circ \epsilon \circ L : R \circ L \circ R \circ L \Longrightarrow R \circ 1_{\mathbf{D}} \circ L = R \circ L$. We wish to establish the commutativity of the following squares:

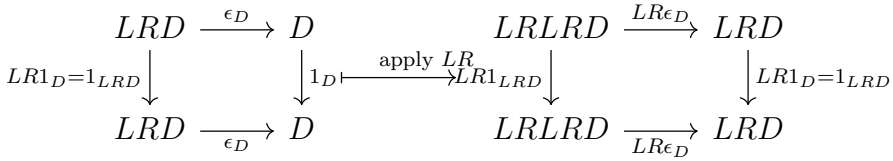




In particular, we first wish to show

$$R \circ \epsilon \circ L \circ R \circ \epsilon \circ L \circ R \circ L = R \circ \epsilon \circ L \circ R \circ L \circ R \circ \epsilon \circ L.$$

For this, remember that ϵ is the counit of $R \vdash L$ and in particular, a natural transformation. So for $1_D : D \to D$ in $\mathbf{D}$, we have the following implication (remember that functor preserves commutativity of a diagram, because it's a functor):



But we also know that (or can see easily) if we have an endofunctor $F : \mathbf{D} \longrightarrow \mathbf{D}$ and a nat. trans. $\epsilon : F \Longrightarrow 1_{\mathbf{D}}$, then the composite nat. trans. $\epsilon \circ F$ and $F \circ \epsilon$ are same. Thus in our case $LR \circ \epsilon_D = \epsilon_{LRD}$, thus giving us the first commutativity. For second, we need to show that

$$R \circ \epsilon \circ L \circ \eta \circ R \circ L = 1_{R \circ L} = R \circ \epsilon \circ L \circ R \circ L \circ \eta.$$

To show that they both are equal to $1_{R \circ L}$, we simply see that the following triangles commute because of zig-zag identities of $R \vdash L$:

and then to, say the diagram on the right, apply R to get $R \circ \epsilon \circ L \circ R \circ L \circ \eta = R \circ 1_L = 1_{R \circ L}$. ■

4.1 Algebras over a monad

The Lemma 4.0.3 tells us that if we have an adjunction, then we have a monad on the source of it's left adjoint. We will now learn about it's converse, that is, from a monad, we will construct an adjunction on that category whose left adjoint will have this category as the source. This construction would need to first define the other category of the adjunction. As we will see, this category is quite interesting.

> ***Main goal of this subsection :*** To establish that each monad gives an adjunction via the construction of Eilenberg-Moore categories, Theorem 10.

We begin with defining algebras over a monad:

Definition 4.1.1. (**Algebra over a Monad**) *Let $\boldsymbol{C}$ be a category and $(\mathbb{T}, \eta, \mu)$ be a monad over $\boldsymbol{C}$. We then define a $\mathbb{T}$-algebra to be a pair of information (C, h) where C is an object and $h : \mathbb{T}C \longrightarrow C$ is an arrow of $\boldsymbol{C}$, which renders the following diagrams commutative:*

$$\begin{array}{ccc} \mathbb{T}\mathbb{T}C & \xrightarrow{\mathbb{T}h} & \mathbb{T}C \\ {\scriptstyle \mu_C}\downarrow & & \downarrow{\scriptstyle h} \\ \mathbb{T}C & \xrightarrow[h]{} & C \end{array} \qquad \text{Associativity}$$

$$\begin{array}{ccc} C & \xrightarrow{\eta_C} & \mathbb{T}C \\ & {\scriptstyle 1_C}\searrow & \downarrow{\scriptstyle h} \\ & & C \end{array} \qquad \text{Unitality}$$

*The object C is called the **underlying object** and the arrow h is called the **structure map** of the $\mathbb{T}$-algebra (C, h).*

We can then naturally define a morphism between two $\mathbb{T}$-algebras:

Definition 4.1.2. (**Morphism of $\mathbb{T}$-Algebras**) *Let $\boldsymbol{C}$ be a category and $(\mathbb{T}, \eta, \mu)$ be a monad over $\boldsymbol{C}$. Also let (C, h) and (C', h') be two $\mathbb{T}$-algebras. An arrow $f : C \longrightarrow C'$ in $\boldsymbol{C}$ is defined to be a morphism $f : (C, h) \longrightarrow (C', h')$ of $\mathbb{T}$-algebras if the following square commutes:*

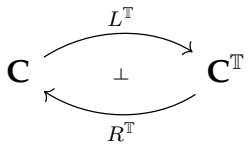
$$\begin{array}{ccc} \mathbb{T}C & \xrightarrow{h} & C \\ {\scriptstyle \mathbb{T}f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathbb{T}C' & \xrightarrow[h']{} & C' \end{array}.$$

Remark 4.1.3. (**Category of $\mathbb{T}$-Algebras/Eilenberg-Moore Category**) Let $(\mathbb{T}, \eta, \mu)$ be a monad over $\mathbf{C}$. We can then construct the category of all $\mathbb{T}$-algebras as objects and $\mathbb{T}$-algebra morphisms as arrows. This category is was first constructed by Eilenberg & Moore in their classic 1965 paper, and hence is named after them. We denote this category by

$$\mathbf{C}^{\mathbb{T}}.$$

We then have the following result:

Theorem 10. (*Eilenberg-Moore*) Let $(\mathbb{T}, \eta, \mu)$ be a monad over a category $\mathbf{C}$ and denote by $\mathbf{C}^{\mathbb{T}}$ the category of all $\mathbf{T}$-algebras. Then, there is an adjunction



where

$$\begin{aligned} L^{\mathbb{T}} : \mathbf{C} &\longrightarrow \mathbf{C}^{\mathbb{T}} \\ C &\longmapsto (\mathbb{T}C, \mu_C : \mathbb{T}(\mathbb{T}C) \to \mathbb{T}C) \\ f : C \to C' &\longmapsto \mathbb{T}f : \mathbb{T}C \to \mathbb{T}C' \end{aligned}$$

and

$$\begin{aligned} R^{\mathbb{T}} : \mathbf{C}^{\mathbb{T}} &\longrightarrow \mathbf{C} \\ (C, h) &\longmapsto C \\ f : (C, h) \to (C', h') &\longmapsto f : C \to C'. \end{aligned}$$

The unit of this adjunction $\eta^{\mathbb{T}} : 1_{\mathbf{C}} \Longrightarrow R^{\mathbb{T}} \circ L^{\mathbb{T}}$ is equal to the unit η of the monad and the counit $\epsilon^{\mathbb{T}} : L^{\mathbb{T}} \circ R^{\mathbb{T}} \Longrightarrow 1_{\mathbf{C}^{\mathbb{T}}}$ is given by components

$$\begin{aligned} &\epsilon^{\mathbb{T}}_{(C,h)} : L^{\mathbb{T}} \circ R^{\mathbb{T}}(C, h) = (\mathbb{T}C, \mu_C) \longrightarrow (C, h) \\ &= h : (\mathbb{T}C, \mu_C) \longrightarrow (C, h). \end{aligned}$$

Proof. We first need to verify that each of the mappings $L^{\mathbb{T}}$ and $R^{\mathbb{T}}$ indeed are valid functors. We only need to verify for $L^{\mathbb{T}}$ as $R^{\mathbb{T}}$ is simply the forgetful functor. For $L^{\mathbb{T}}$, we need to see whether the following diagrams commute:

and it's not difficult to see that they indeed do commute because $\mathbb{T}$ is a monad.

We next need to verify that $\epsilon^{\mathbb{T}}$ and $\eta^{\mathbb{T}}$ as described are indeed natural transformations. This is very trivial.

We will now prove the adjunction $R^{\mathbb{T}} \vdash L^{\mathbb{T}}$. For this, we'll use the zig-zag identity. Hence, we wish to show that the following commutes:

that is, we have to show that the following: take any $(C, h) \in \mathbf{C}^{\mathbb{T}}$, we then need to show that

$$(R^{\mathbb{T}}\epsilon^{\mathbb{T}} \circ \eta^{\mathbb{T}}R^{\mathbb{T}})_{(C,h)} = 1_{R^{\mathbb{T}}(C,h)} = 1_C$$

and this can be established as follows:

$$\begin{aligned}(R^{\mathbb{T}}\epsilon^{\mathbb{T}})_{(C,h)} \circ (\eta^{\mathbb{T}}R^{\mathbb{T}})_{(C,h)} &= h \circ \eta_C \\ &= 1_C\end{aligned}$$

where last equation follows from unitality of a $\mathbb{T}$-algebra. Next, we need to show that

$$\left(\epsilon^{\mathbb{T}}L^{\mathbb{T}} \circ L^{\mathbb{T}}\eta^{\mathbb{T}}\right)_C = 1_{L^{\mathbb{T}}C} = 1_{\mathbb{T}C}$$

which can again be observed simply as follows

$$\begin{aligned}(\epsilon^{\mathbb{T}}L^{\mathbb{T}})_C \circ (L^{\mathbb{T}}\eta^{\mathbb{T}})_C &= \mu_C \circ \mathbb{T}\eta_C \\ &= 1_{\mathbb{T}C}\end{aligned}$$

where last equation follows from right unitality of monad $\mathbb{T}$. Moreover, the process of Lemma 4.0.3 to derive a monad from an adjunction, as expected, gives us the same monad back in this case, that is

$$\begin{aligned}R^{\mathbb{T}} \circ L^{\mathbb{T}}(C) &= R^{\mathbb{T}}\left((\mathbb{T}C, \mu_C)\right) = \mathbb{T}C \\ \eta^{\mathbb{T}} &= \eta \\ R^{\mathbb{T}} \circ \epsilon^{\mathbb{T}} \circ L^{\mathbb{T}}(C) &= R^{\mathbb{T}}\left(\epsilon^{\mathbb{T}}(\mathbb{T}C, \mu_C)\right) \\ &= R^{\mathbb{T}}\left(\epsilon^{\mathbb{T}}_{(\mathbb{T}C,\mu_C)}\right) \\ &= R^{\mathbb{T}}(\mu_C) \\ &= \mu_C\end{aligned}$$

which shows that we indeed get our monad back. Hence proved. ■

It is only beneficial if we look at some of the examples of $\mathbb{T}$-algebras:

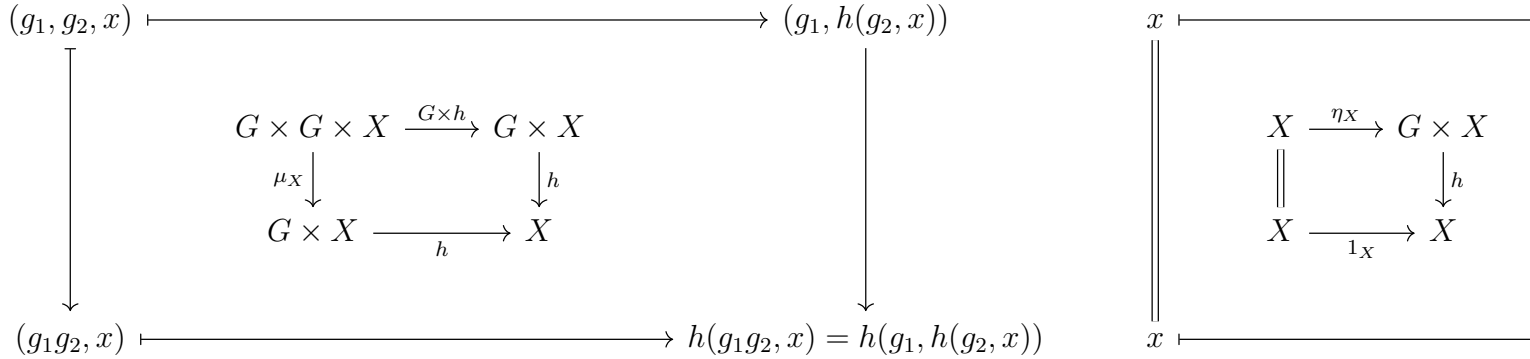
Example. (**G-sets as algebras over a monad**) Let G be a group. Consider the monad $\mathbb{G} : \mathbf{Sets} \longrightarrow \mathbf{Sets}$, $X \longmapsto G \times X$ with unit and multiplication natural maps as

$$\begin{aligned}\eta : 1_{\mathbf{Sets}} &\Longrightarrow \mathbb{G} \\ \eta_X : X &\longrightarrow G \times X \\ x &\longmapsto (1, x)\end{aligned}$$

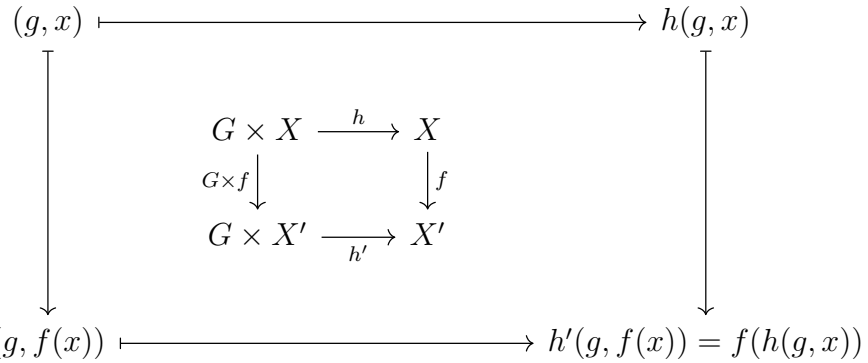
and

$$\begin{aligned}\mu : \mathbb{G} \circ \mathbb{G} &\Longrightarrow \mathbb{G} \\ \mu_X : G \times (G \times X) &\longrightarrow G \times X \\ (g_1, g_2, x) &\longmapsto (g_1 g_2, x).\end{aligned}$$

It can be seen quite easily that the natural maps defined above indeed gives a monad $(\mathbb{G}, \eta, \mu)$ (the two diagrams for a monad just establishes the associativity and left/right unitality of G's action). Now consider a $\mathbb{G}$-algebra in **Sets**, denoted (X, h) where X is a set and $h : G \times X \longrightarrow X$ is the structure map. By the definition of a $\mathbb{G}$-algebra it must satisfy the following squares:



which tells us that a $\mathbb{G}$-algebra is just a G-set. Moreover, let (X', h') be another $\mathbb{G}$-algebra. Then, a $\mathbb{G}$-algebra morphism $f : (X, h) \longrightarrow (X', h')$ is the map $f : X \longrightarrow X'$ in **Sets** satisfying the following diagram:



which, as expected, tells us that f is a G-morphism between G-sets. Moreover, any G-set X can also be written as a particular $\mathbb{G}$-algebra; the pair (X, h) where $h : G \times X \longrightarrow X$ is the G-action on X defines a $\mathbb{G}$-algebra as it satisfies both the above squares. Hence, the category of all $\mathbb{G}$-algebras (or, Eilenberg-Moore category of $\mathbb{G}$) is just isomorphic to the category of all G-sets, that is,

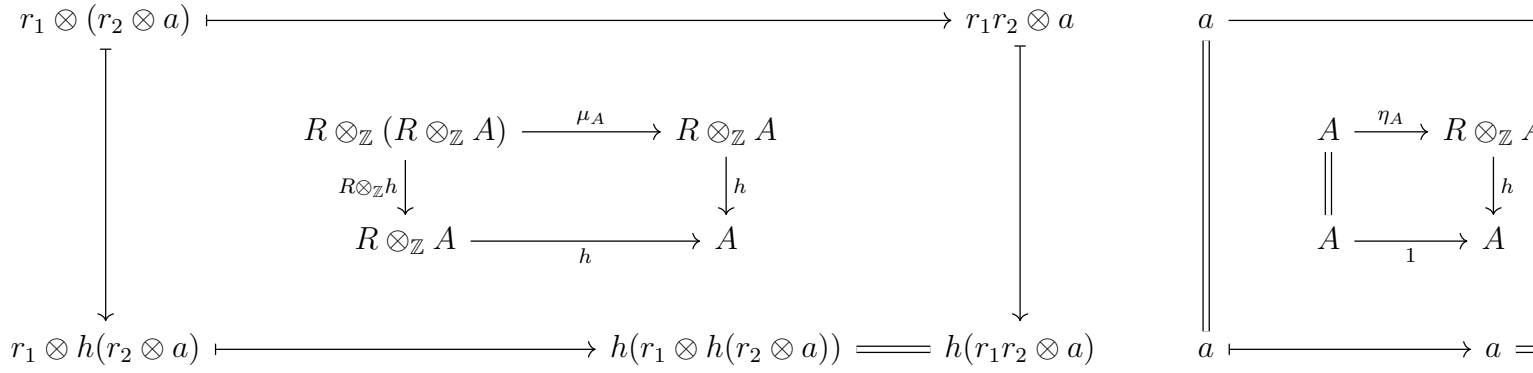
$$\mathbf{Sets}^{\mathbb{G}} \cong G - \mathbf{Sets}.$$

Another interesting example is that of a monad whose algebras are exactly the R-modules for a ring R:

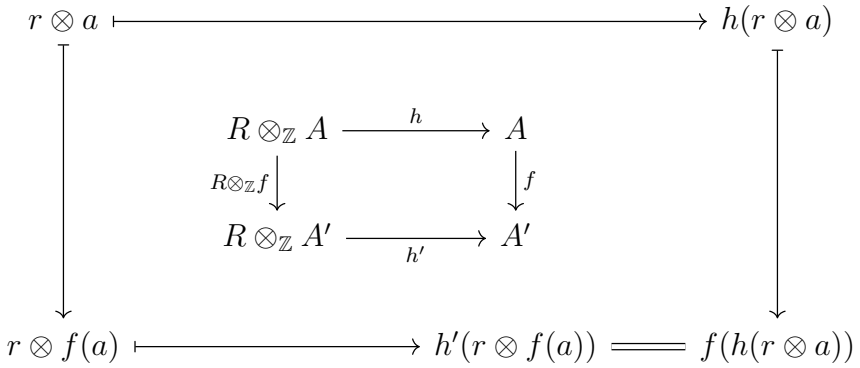
Example. (***R*-modules as algebras over a monad**) Consider the category **AbGrp** of abelian groups and homomorphisms and let R be a ring. Remember that the ring R can be denoted as a $\mathbb{Z}$-algebra (in particular, a $\mathbb{Z}$-module) and similarly an abelian group A is a $\mathbb{Z}$-module. Define the following monad over **AbGrp**:

$$\begin{aligned}
\mathbb{T} : \mathbf{AbGrp} &\longrightarrow \mathbf{AbGrp} \\
A &\longmapsto R \otimes_{\mathbb{Z}} A \\
\eta : 1_{\mathbf{AbGrp}} &\Longrightarrow \mathbb{T} \\
\eta_A : A &\longrightarrow R \otimes_Z A \\
a &\longmapsto 1 \otimes a \\
\mu : \mathbb{T} \circ \mathbb{T} &\Longrightarrow \mathbb{T} \\
\mu_A : R \otimes_{\mathbb{Z}} (R \otimes_{\mathbb{Z}} A) &\longrightarrow R \otimes_{\mathbb{Z}} A \\
r_1 \otimes (r_2 \otimes a) &\longmapsto (r_1 r_2) \otimes a
\end{aligned}$$

The fact that this indeed is a monad can be seen quite easily (those diagrams just establish the associativity and left/right unitality of $\otimes$). Now, consider a $\mathbb{T}$-algebra (A, h) where A is an abelian group and $h : R \otimes_{\mathbb{Z}} A \longrightarrow A$ is the structure map. Again, by definition of $\mathbb{T}$-algebra, we must have the following commuting squares:



The squares then gives us a $\mathbb{Z}$-module homomorphism $h : R \otimes_{\mathbb{Z}} A \longrightarrow A$ because $h(r_1 \otimes a_1 + r_2 \otimes a_2) = h(r_1 \otimes a_1) + h(r_2 \otimes a_2)$ follows already as $R \otimes_{\mathbb{Z}} A$ is in **AbGrp**. Similarly, $h(n(r \otimes a)) = nh(r \otimes a)$ as $n(r \otimes a)$ is defined to be $r \otimes a + \ldots r \otimes a$ total n times. With this $\mathbb{Z}$-module homomorphism h, we then have that the composite with structure map h gives us $R \times A \longrightarrow R \otimes_{\mathbb{Z}} A \longrightarrow A$ which is a bilinear mapping and thus defines A to be a R-module. Conversely, any R-module A has a bilinear map $R \times A \longrightarrow A$ which thus extends to a structure map $h : R \otimes_{\mathbb{Z}} A \longrightarrow A$, hence giving us a $\mathbb{T}$-algebra (A, h). Thus all $\mathbb{T}$-algebras are left R-modules.
Moreover, let (A', h') be another $\mathbb{T}$-algebra and $f : (A, h) \longrightarrow (A', h')$ be a morphism between $\mathbb{T}$-algebras in **AbGrp**. We thus have that the following commutes



which defines simply an R-module homomorphism. Hence we have the following isomorphism of categories:

$$\mathbf{AbGrp}^{\mathbb{T}} \cong R - \mathbf{Mod}.$$

We now come to our main motivation for introducing monads, that is to introduce monadic functors.

4.2 Monadicity

Let $L : \mathbf{C} \rightleftarrows \mathbf{D} : R$ be a given adjunction. By Lemma 4.0.3, we can construct a monad over $\mathbf{C}$ given by $(R \circ L, \eta, R \circ \epsilon \circ L)$. Moreover, by Theorem 10, we can convert this monad on $\mathbf{C}$ to an adjunction $\mathbf{C} \rightleftarrows \mathbf{C}^{\mathbb{T}}$. A natural question to ask now is the following: How much information does this adjunction $\mathbf{C} \rightleftarrows \mathbf{C}^{\mathbb{T}}$ stores about the original adjunction $L : \mathbf{C} \rightleftarrows \mathbf{D} : R$? The answer is that the information about original adjunction is preserved upto a unique functor, as we will soon see.

> ***Main goal of this subsection :*** To establish comparison between a given adjunction and the algebras of the monad derived from it, Theorem 11.

Let us first remind ourselves on the notion of transformation of one adjoint to the other:

Definition 4.2.1. (**Morphism of Adjoints**) *Let $L : \boldsymbol{C} \rightleftarrows \boldsymbol{D} : R$ and $L' : \boldsymbol{C'} \rightleftarrows \boldsymbol{D'} : R'$ be two adjunctions. A morphism of above adjunctions is given by a pair of functors $J : \boldsymbol{C} \longrightarrow \boldsymbol{C'}$, $K : \boldsymbol{D} \longrightarrow \boldsymbol{D'}$ satisfying the following two axioms:*

1. *The following squares commute*

$$\begin{array}{ccc} \mathbf{C} & \xrightarrow{L} & \mathbf{D} \\ {\scriptstyle J}\downarrow & & \downarrow{\scriptstyle K} \\ \mathbf{C'} & \xrightarrow[L']{} & \mathbf{D'} \end{array} \qquad \begin{array}{ccc} \mathbf{C} & \xleftarrow{R} & \mathbf{D} \\ \downarrow{\scriptstyle J} & & \downarrow{\scriptstyle K} \\ \mathbf{C'} & \xleftarrow[R']{} & \mathbf{D'} \end{array}.$$

   That is, $K \circ L = L' \circ J$ and $J \circ R = R' \circ K$.

2. *The following square commutes*

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathbf{D}}(LC, D) & \xrightarrow{\cong} & \mathrm{Hom}_{\mathbf{C}}(C, RD) \\
{\scriptstyle K(-)}\downarrow & & \downarrow{\scriptstyle J(-)} \\
\mathrm{Hom}_{\mathbf{D}'}(KLC, KD) & & \mathrm{Hom}_{\mathbf{C}'}(JC, JRD) \\
\| & & \| \\
\mathrm{Hom}_{\mathbf{D}'}(L'JC, KD) & \xrightarrow[\cong]{} & \mathrm{Hom}_{\mathbf{C}'}(JC, R'KD)
\end{array} .$$

With this, we next prove a result which says that there is a simpler equivalent condition which we can write in place of axiom 2 of Definition 4.2.1 above:

Proposition 4.2.2. Consider two adjunctions $\eta, L : \mathbf{C} \rightleftarrows \mathbf{D} : R, \epsilon$ and $\eta', L' : \mathbf{C}' \rightleftarrows \mathbf{D}', : R', \epsilon'$. Let $(J : \mathbf{C} \to \mathbf{C}', K : \mathbf{D} \to \mathbf{D}')$ be a morphism of adjunctions $(J, K) : R \vdash L \rightrightarrows R' \vdash L'$. Then we have the following equality between natural transforms:

$$\begin{array}{ccc}
J & \xrightarrow{J\eta} & JRL \\
\| & & \| \\
J & \xrightarrow[\eta' J]{} & R'L'J
\end{array} \qquad
\begin{array}{ccc}
KLR & \xrightarrow{K\epsilon} & K \\
\| & & \| \\
L'R'K & \xrightarrow[\epsilon' K]{} & K
\end{array} .$$

That is, $\eta' J = J\eta$ and $\epsilon' K = K\epsilon$.

Proof. Take any object C of $\mathbf{C}$. We then have that $J\eta_C : JC \longrightarrow JRLC$. Similarly, we have $\eta' JC = \eta'_{JC} : JC \longrightarrow R'L'JC$. Since the pair of functors (J, K) forms an adjoint morphism, therefore from axiom 2 of Definition 4.2.1 with $D := LC$, we get the following if we follow the arrow 1_{LC} around:

$$\begin{array}{ccccc}
LC & \xrightarrow{1} & LC & \longmapsto & C \xrightarrow{\eta_C} RLC \\
\downarrow & & & & \downarrow \\
KLC & \xrightarrow{1} & KLC & & JC \xrightarrow{J\eta_C} JRLC \\
\| & & & & \| \\
L'JC & \xrightarrow{1} & L'JC \longmapsto JC & \xrightarrow{\eta'_{JC}} R'KLC = & JC \xrightarrow{J\eta_C} R'KLC
\end{array}$$

This establishes that the components of $J\eta$ and $\eta' J$ are same, and thus proves the result. Similarly, one can show that $\epsilon' K = K\epsilon$ by using diagram of axiom 2 but using $C := RD$ and chasing ϵ_D around. ■

We then have the theorem establishing the fact that one can get back the data of original adjunction upto a unique functor by looking at the category of algebras of the monad derived from the given adjunction:

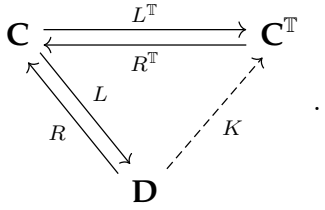
Theorem 11. Let the following be a given adjunction

$$\mathbf{C} \underset{R}{\overset{L}{\rightleftarrows}} \mathbf{D} \quad (\perp)$$

with ϵ, η denoting it's counit-unit pair and denote the monad on $\mathbf{C}$ given by Lemma 4.0.3 as $\mathbb{T} = (R \circ L, \eta, R \circ \epsilon \circ L)$. Moreover, denote the adjunction then derived from this monad via Theorem 10 as the following

$$\mathbf{C} \underset{R^{\mathbb{T}}}{\overset{L^{\mathbb{T}}}{\rightleftarrows}} \mathbf{C}^{\mathbb{T}} \quad (\perp) .$$

Then there exists a unique functor $K : \mathbf{D} \longrightarrow \mathbf{C}^{\mathbb{T}}$, called the *comparison functor*, such that the following commutes



That is, $K \circ L = L^{\mathbb{T}}$ and $R^{\mathbb{T}} \circ K = R$.

Proof. Define K as follows:

$$\begin{aligned} K : \mathbf{D} &\longrightarrow \mathbf{C}^{\mathbb{T}} \\ D &\longmapsto (RD, R\epsilon_D := RLRD \to RD) \\ g : D \to D' &\longmapsto (Rg)^{\mathbb{T}} : (RD, R\epsilon_D) \to (RD', R\epsilon_{D'}). \end{aligned}$$

Note that $(Rg)^{\mathbb{T}}$ is simply the arrow Rg in $\mathbf{C}$ but is interpreted as a morphism of monads. That being said, we first need to show that this is well-defined, that is, the map $(Rg)^{\mathbb{T}}$ is indeed a $\mathbb{T}$-algebra morphism. For this, we wish to establish commutativity of the following diagram:

$$\begin{array}{ccc} RLRD & \xrightarrow{RLRg} & RLRD' \\ {\scriptstyle R\epsilon_D}\downarrow & & \downarrow{\scriptstyle R\epsilon_{D'}} \\ RD & \xrightarrow[Rg]{} & RD' \end{array}.$$

For this, note that by the adjunction property, we have the following triangle for the arrow $g \circ \epsilon_D : LRD \to D'$ in $\mathbf{D}$:

$$\begin{array}{ccc} & & LRD \\ & {\scriptstyle g\circ\epsilon_D}\swarrow & \downarrow{\scriptstyle L(Rg)} \\ D' & \xleftarrow[\epsilon_{D'}]{} & LRD' \end{array}.$$

Thus, if we apply R on the above commutative triangle, we get $R(g \circ \epsilon_D) = Rg \circ R\epsilon_D = R\epsilon_{D'} \circ RLRg$ and this is what we wanted. We next need to show that this is indeed a functor. For this, take any $g_1 : D_1 \to D_2$ and $g_2 : D_2 \to D_3$ in $\mathbf{D}$. Drawing their corresponding $\mathbb{T}$ algebra morphism squares establishes that indeed $(Rg_2)^{\mathbb{T}} \circ (Rg_1)^{\mathbb{T}} = (R(g_2 \circ g_1))^{\mathbb{T}}$. Next, we wish to show that K as defined satisfies all the required hypotheses. This follows from the following:

$$\mathbf{C} \xrightarrow{L} \mathbf{D} \xrightarrow{K} \mathbf{C}^{\mathbb{T}} \qquad\qquad \mathbf{D} \xrightarrow{K} \mathbf{C}^{\mathbb{T}} \xrightarrow{R^{\mathbb{T}}} \mathbf{C}$$

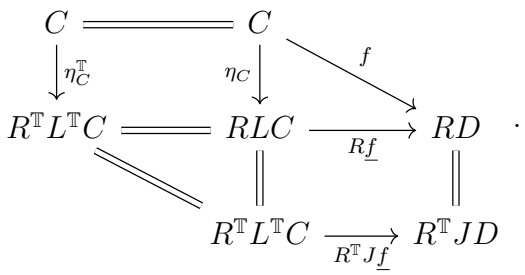
$$C \longmapsto LC \longmapsto (RLC, R\epsilon_{LC}) \qquad\qquad D \longmapsto (RD, \epsilon_D) \longmapsto RD \ .$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad$$

$$L^{\mathbb{T}}C := (RLC, R\epsilon L(C))$$

Hence, the K defined as above satisfies all the hypotheses. Finally, we wish to show that this K is unique. For this, take any other functor $J : \mathbf{D} \longrightarrow \mathbf{C}^{\mathbb{T}}$ which also satisfies $J \circ L = L^{\mathbb{T}}$ and $R^{\mathbb{T}} \circ J = R$. We wish to show that $J = K$. Let us first show that the underlying object of JD is indeed equal to that of $KD = (RD, R\epsilon_D)$. For this, since $R^{\mathbb{T}} \circ J(D) = RD$ and $R^{\mathbb{T}}$ is just the forgetful functor, therefore indeed the underlying object of JD is RD. Next, we show that the structure map of JD is same as KD, i.e. structure map of JD is $R\epsilon_D : RLRD \to RD$. For this, we first note that the pair $\left(1_{\mathbf{C}} : \mathbf{C} \to \mathbf{C} :, J : \mathbf{D} \to \mathbf{C}^{\mathbb{T}}\right)$ is

a morphism of adjunctions; the fact that both squares in Definition 4.2.1, 1 commutes follows trivially because $J \circ L = L^{\mathbb{T}} \circ 1_{\mathbf{C}}$ and $1_{\mathbf{C}} \circ R = R^{\mathbb{T}} \circ J$ holds because of hypotheses, the square in Definition 4.2.1, 2 commutes because $R^{\mathbb{T}} \vdash L^{\mathbb{T}}$ and $R \vdash L$ both have the same unit η, so in the following diagram, we will have that $R^{\mathbb{T}} J\underline{f} \circ \eta_C = f$, thus $J\underline{f} = \underline{f}$, which means that it commutes:



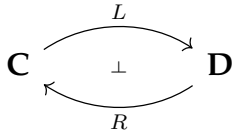
So indeed $(1_{\mathbf{C}}, J)$ is an adjoint morphism. Hence, by Proposition 4.2.2, we have that $\epsilon^{\mathbb{T}} J = J\epsilon$. This means that for any object D in $\mathbf{D}$, we have

$$\begin{aligned} J\epsilon_D : JLRD \to JD &= \epsilon^{\mathbb{T}}_{JD} : L^{\mathbb{T}}R^{\mathbb{T}}JD \to JD \\ &= \text{Structure map of } JD \text{ (See Theorem 10).} \end{aligned}$$

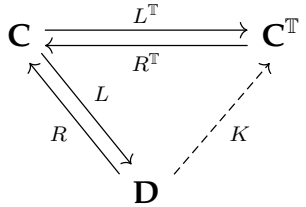
Now, note that the functor J takes arrows of $\mathbf{D}$ to what R takes it to; for any $g : D \to D'$ in $\mathbf{D}$, $R^{\mathbb{T}}(Kg) = Rg$ and $R^{\mathbb{T}}$ is simply the forgetful functor. Therefore, $J\epsilon_D = R\epsilon_D$, proving that J is same as K. ■

We finally come to the definition of a monadic functor:

Definition 4.2.3. (**Monadic Functor**) *Let the following be a given adjunction:*



with ϵ, η being the counit-unit pair of this adjunction. Let $\mathbb{T} := (R \circ L, \eta, R \circ \epsilon \circ L)$ be the monad on $\boldsymbol{C}$ derived from this adjunction in Lemma 4.0.3 and let $L^{\mathbb{T}} : \boldsymbol{C} \rightleftarrows \boldsymbol{D} : R^{\mathbb{T}}$ be the adjunction derived in Theorem 10. We then say that the right adjoint $R : \boldsymbol{D} \longrightarrow \boldsymbol{C}$ is a monadic functor if the unique comparison functor $K : \boldsymbol{D} \longrightarrow \boldsymbol{C}^{\mathbb{T}}$ as in



from Theorem 11 is an isomorphism.

Remark 4.2.4. As showed by Theorem 11, the functor K is simply the mapping

$$\begin{aligned} K : \mathbf{D} &\longrightarrow \mathbf{C}^{\mathbb{T}} \\ D &\longmapsto (RD, R\epsilon_D) \\ (g : D \to D') &\longmapsto (Rg : (RD, R\epsilon_D) \to (RD', R\epsilon_{D'})) \end{aligned}$$

so to establish the monadicity of R, we just need to show that this mapping of $\mathbf{D}$ into the category of algebras $\mathbf{C}^{\mathbb{T}}$ is an isomorphism. This can only happen when the adjunction we began with, $R \vdash L$, gives us the monad $\mathbb{T}$ whose category of algebras $\mathbf{C}^{\mathbb{T}}$ is same upto an isomorphism to $\mathbf{D}$.
In particular, if R is monadic, then the adjunctions $R \vdash L$ and $R^{\mathbb{T}} \vdash L^{\mathbb{T}}$ are isomorphic. Moreover, each $\mathbb{T}$-algebra (C, h) in $\mathbf{C}^{\mathbb{T}}$ is isomorphic to/of the form $(RD, R\epsilon_D)$ for some object D of $\mathbf{D}$.

4.3 Beck's monadicity theorem

We will now look at a very useful criterion to determine when a functor is monadic. This will reap fruits in our discussion on categorical Galois theory, in particular, on monadic descent.

> ***Main goal of this subsection :*** To establish Beck's Monadicity Theorem to characterize monadic adjunctions, Theorem 12.

Let us first describe some terminology regarding split forks:

Definition 4.3.1. (**Retracts**) *Let $\boldsymbol{C}$ be a category. An arrow $f : X \to Y$ is said to be a retract of $g : X' \to Y'$ if the following diagram commutes*

$$\begin{array}{ccccc} X & \longrightarrow & X' & \longrightarrow & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle f} \\ Y & \longrightarrow & Y' & \longrightarrow & Y \end{array}$$

where both the horizontal arrows compose to identity on X.

Example. Let $A \subseteq X$ be a subspace of a topological space X. Let $r : X \to A$ be a retraction of A to X. This means that the following commutes:

$$\begin{array}{ccccc} A & \xrightarrow{i} & X & \xrightarrow{r} & A \\ {\scriptstyle 1_A}\downarrow & & \downarrow{\scriptstyle 1_X} & & \downarrow{\scriptstyle 1_A} \\ A & \xrightarrow[i]{} & X & \xrightarrow[r]{} & A \end{array}.$$

Thus, a retraction $r : X \to A$ gives a retract in **Top**. In particular, 1_A is a retract of 1_X whenever such an r exists.

Definition 4.3.2. (**Split Forks**) *Consider the following diagram (also called a fork) in some category $\boldsymbol{C}$:*

$$A \underset{d_1}{\overset{d_0}{\rightrightarrows}} B \xrightarrow{e} C \ .$$

We say that the above diagram is a split fork if there exists arrows

$$A \xleftarrow{t} B \xleftarrow{s} C$$

which makes e the retract of d_1 by the following diagram:

$$\begin{array}{ccccc} B & \xrightarrow{t} & A & \xrightarrow{d_0} & B \\ \downarrow{\scriptstyle e} & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle e} \\ C & \xrightarrow[s]{} & B & \xrightarrow[e]{} & C \end{array}.$$

In particular, the following relations makes the above fork a split fork:

$$e \circ d_0 = e \circ d_1 \ , \ \ e \circ s = 1_C \ , \ \ s \circ e = d_1 \circ t \ , \ \ d_0 \circ t = 1_B.$$

We then have that each split fork is a coequalizer diagram:

Lemma 4.3.3. Let $\mathbf{C}$ be a category in which there is a split fork

$$A \underset{d_1}{\overset{d_0}{\rightrightarrows}} B \xrightarrow{e} C$$

with the arrows $C \xrightarrow{s} B \xrightarrow{t} A$. Then, the above diagram is a coequalizer diagram, i.e. e is the coequalizer of d_0 and d_1.

Proof. Take any $f : B \to D$ such that $f \circ d_0 = f \circ d_1$. We wish to get a unique arrow $k : C \to D$ such that $f = k \circ e$. For this, consider the arrow $f \circ s : C \to D$. This arrow satisfies the following : $(f \circ s) \circ e = f \circ (s \circ e) = f \circ (d_1 \circ t) = f \circ (d_0 \circ t) = f \circ 1_B = f$. To show uniqueness of $f \circ s$, consider any other $k : C \to D$ such that $k \circ e = f$. But then $(k \circ e) \circ s = f \circ s$ and $k \circ (e \circ s) = k$. Hence $f \circ s$ is unique, thus making e the coequalizer of d_0 and d_1. ■

Remark 4.3.4. In particular, every split fork is a coequalizer diagram whose coequalizing arrow is not only epimorphic, but split epimorphic (has a right inverse).

Remark 4.3.5. (**Split forks are always preserved by functors**) It is easy to see that a split fork is preserved by any functor. Hence the split coequalizer of any split fork is a special coequalizer diagram in the sense that it is preserved by any functor. Such coequalizers are called ***absolute***.
For a spit fork, the coequalizing arrow is usually called the ***split coequalizer***.

We now state the Beck's theorem which characterizes the monadic adjunctions:

Theorem 12. (**Beck's Monadicity Theorem**) Let the following be a given adjunction:

$$\mathbf{C} \underset{R}{\overset{L}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} \mathbf{D}$$

whose counit-unit pair is ϵ-η. Denote the monad derived from $R \vdash L$ as

$$\mathbb{T} := (RL, \eta, R\epsilon L)$$

and the consequent adjunction derived from $\mathbb{T}$ as

$$\mathbf{C} \underset{R^{\mathbb{T}}}{\overset{L^{\mathbb{T}}}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} \mathbf{C}^{\mathbb{T}} \ .$$

Finally, denote the comparison functor between the above two adjunctions as $K : \mathbf{D} \longrightarrow \mathbf{C}^{\mathbb{T}}$, $D \longmapsto (RD, R\epsilon_D)$. Then the following conditions are equivalent:

1. K is an isomorphism, making $R : \mathbf{D} \longrightarrow \mathbf{C}$ ***monadic***.
2. Right adjoint $R : \mathbf{D} \longrightarrow \mathbf{C}$ creates coequalizers of those $f, g : D \rightrightarrows D'$ in $\mathbf{D}$ for which the image $Rf, Rg : RD \rightrightarrows RD'$ has an ***absolute coequalizer*** in $\mathbf{C}$.
3. Right adjoint $R : \mathbf{D} \longrightarrow \mathbf{C}$ creates coequalizers for those $f, g : D \rightrightarrows D'$ in $\mathbf{D}$ for which the image $Rf, Rg : RD \rightrightarrows RD'$ has a ***split coequalizer***/is a ***split fork*** in $\mathbf{C}$.

5 The categorical Galois theory

With the motivations and a good suite of examples of classical Galois theories in place, we now study the abstract Galois theorem of Janelidze, which encompasses all of the ones which we have studied so far. This will, in particular, encompass the Galois theory of commutative rings, which we will study in detail as a particular example of this general theorem.

Main goal of this section : To state the abstract Galois theorem.

The following is a general lemma from category theory which tells us that each adjunction restricts to slice to give a particular type of change of base adjunction. This will prove useful in the oncoming discussion:

Lemma 5.0.1. Let the following be a given adjunction where $\mathbf{C}$ has pullbacks:

$$\mathbf{C} \underset{R}{\overset{L}{\rightleftarrows}} \mathbf{D} \ .$$

Let ϵ-η denote it's counit-unit pair. Consider an object C in $\mathbf{C}$. We then have a functor

$$\begin{aligned} L|_{\mathbf{C}/C} : \mathbf{C}/C &\longrightarrow \mathbf{D}/LC \\ (X, f : X \to C) &\longmapsto (LX, Lf : LX \to LC) \\ g : (X, f) \to (X', f') &\longmapsto Lg : (LX, Lf) \to (LX', Lf'). \end{aligned}$$

Then, this functor has a right adjoint given by pulling back along the unit at C the image of R, i.e.

$$\eta_C^* R(-) \quad : \quad \mathbf{D}/LC \longrightarrow \mathbf{C}/C$$

$$\begin{array}{ccc} Y & & \eta_C^*(Rg) \xrightarrow{\pi_2} RY \\ {\scriptstyle g}\downarrow & \longrightarrow & \circlearrowright_{\pi_1}\downarrow \quad \lrcorner \quad \downarrow{\scriptstyle Rg} \\ LC & & C \xrightarrow[\eta_C]{} RLC \end{array} \ .$$

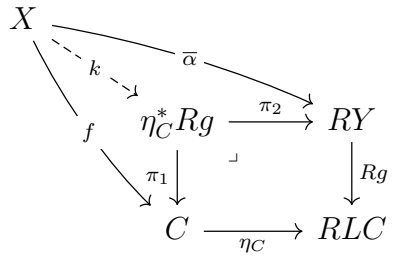
That is, for each adjunction $R \vdash L$ and any $C \in \mathbf{C}$, we have the following adjunction:

$$\mathbf{C}/C \underset{\eta_C^* R(-)}{\overset{L|_{\mathbf{C}/C}}{\rightleftarrows}} \mathbf{D}/LC \ .$$

Proof. Take any $\alpha : L|_{\mathbf{C}/C}(X, f) \longrightarrow (Y, g)$. We will show that the functor $L|_{\mathbf{C}/C}$ as described above is left adjoint to the functor $\eta_C^* R(-)$. This is simply explained by the following diagram:

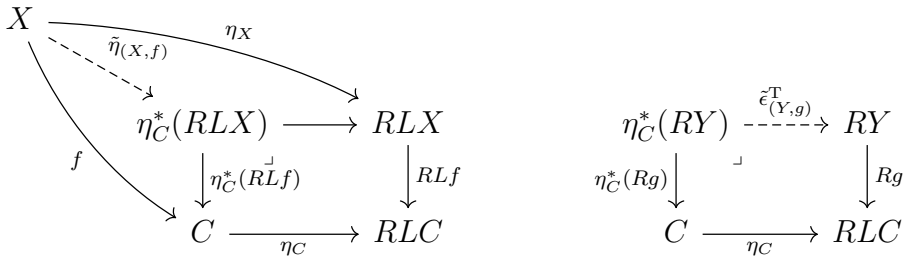
$$\begin{array}{ccc} (LX, Lf) & & \\ {\scriptstyle Lk}\vdots & \searrow^{\alpha} & \\ (L\eta_C^* Rg, L\pi_1) & \xrightarrow[\tilde{\epsilon}_Y := \epsilon_Y \circ L\pi_2]{} & (Y, g) \end{array}$$

where $\eta_C^* Rg$, π_1, π_2 and k are given as in the following pullback diagram:



where the $\overline{\alpha}$ is the right adjoint of $\alpha : LX \to Y$ in $\mathbf{D}$. We also need to show that $Rg \circ \overline{\alpha} = \eta_C \circ f$. To see this, look at their left adjoints and one can see, from the naturality of the unit η and from the fact that $g \circ \alpha = Lf$, that both of them has left adjoint equal to Lf. Hence they must be same by uniqueness of adjunct pairs. This shows that $L|_{\mathbf{C}/C}$ is left adjoint to $\eta_C^* R(-)$. ■

Remark 5.0.2. A bit of fiddling around can tell you the unit ($\tilde{\eta}$) and counit ($\tilde{\epsilon}$) of the above slice adjunction. For an object $(X, f : X \to C)$ of $\mathbf{C}/C$ and $(Y, g : Y \to LC)$ of $\mathbf{D}/LC$, they are as explained in the diagram below:



where $\tilde{\epsilon}^{\mathrm{T}}_{(Y,g)}$ is the transpose of $\tilde{\epsilon}_{(Y,g)}$ by the adjunction $R \vdash L$.

Let us now present the definitions leading up to the abstract Galois theorem. We first define an admissible class of arrows:

Definition 5.0.3. (**Admissible Class**) *Let $\boldsymbol{C}$ be a category. A class of morphisms $A \subseteq \mathrm{Ar}(\boldsymbol{C})$ is called admissible if it satisfies the following conditions:*

1. *Every isomorphism of $\boldsymbol{C}$ is in A.*
2. *A is closed under composition.*
3. *If $C \xrightarrow{f} D \xleftarrow{g} C'$ are in A, then their pullbacks along each other are also in A; A is closed under pullback of any two of it's arrows.*

Example. In **Sets**, consider the collection $A \subset Ar(\mathbf{Sets})$ which consists of all isomorphisms in **Sets**. The 1st and 2nd conditions of Definition 5.0.3 are trivially satisfied. The 3rd condition follows from the fact that in **Sets**, each isomorphism is both a mono and epi and each arrow which is both mono and epi is an iso, and it also holds in **Sets** that pullback of an epi is an epi[31]. Hence, this class A is also closed under pullbacks, thus making A an admissible class of morphisms of **Sets**. In-fact, from the discussion above, the collection of all isomorphisms in any topos **E** is an admissible class of morphisms of **E**.

We next define the admissible class of arrows over a particular object:

Definition 5.0.4. (**Admissible Category over an Object**) *Let $\boldsymbol{C}$ be a category and C be an object of it. Also let $A \subseteq \mathrm{Ar}(\boldsymbol{C})$ be an admissible class of arrows of $\boldsymbol{C}$. Then, we denote A/C to be the admissible category over C which has*

[31] Actually it holds in any topos, see the section on slice topos and change of base functor in [MM92].

1. *Objects as pairs* (X, f) *where* $f : X \to C$ *is in* A.

2. *Arrows as* $g : (X, f) \to (X', f')$ *where* $g : X \to X'$ *is an arrow in* $\boldsymbol{C}$ *such that* $f' \circ g = f$.

Thus, A/C *is a full subcategory of* $\boldsymbol{C}/C$.

Example. In continuation of the example above on admissible class of isomorphic arrows A of **Sets**, for a set X, the admissible category A/X would be the full subcategory of slice **Sets**$/X$ of all those functions which are bijective onto X.

We next define a particular type of adjunction which preserves the admissible classes of both the categories:

Definition 5.0.5. (**Relatively Admissible Adjunction**) *Let* $\boldsymbol{C}$ *and* $\boldsymbol{D}$ *be two categories which have admissible classes* $A_{\boldsymbol{C}} \subseteq \mathrm{Ar}(\boldsymbol{C})$ *and* $A_{\boldsymbol{D}} \subseteq \mathrm{Ar}(\boldsymbol{D})$. *Let the following be a given adjunction between* $\boldsymbol{C}$ *and* $\boldsymbol{D}$*:*

$$\mathbf{C} \underset{R}{\overset{L}{\underset{\curvearrowleft}{\overset{\curvearrowright}{\perp}}}} \mathbf{D} \ .$$

We then define this adjunction $R \vdash L$ *to be relatively admissible for* $A_{\boldsymbol{C}}$ *and* $A_{\boldsymbol{D}}$ *if the following conditions are satisfied:*

1. *If* $f \in A_{\boldsymbol{C}}$, *then* $Lf \in A_{\boldsymbol{D}}$.

2. *If* $g \in A_{\boldsymbol{D}}$, *then* $Rg \in A_{\boldsymbol{C}}$.

3. *The unit* $\eta_C : C \to RLC$ *at any object* C *of* $\boldsymbol{C}$ *is in* $A_{\boldsymbol{C}}$.

4. *The counit* $\epsilon_D : LRD \to D$ *at any object* D *of* $\boldsymbol{D}$ *is in* $A_{\boldsymbol{D}}$.

We next define what we mean by effective descent morphisms relative to an admissible class; these will generalize what we called "field extensions" to this general scenario:

Definition 5.0.6. (**Effective Descent Morphism relative to an Admissible Class**) *Let* $\boldsymbol{C}$ *be a category and* $A \subseteq \mathrm{Ar}(\boldsymbol{C})$ *be an admissible class. A morphism* $\sigma : X \longrightarrow Y$ *in* $\boldsymbol{C}$ *is called an effective descent morphism relative to* A *if* $\sigma \in A$ *and the change of base functor*

$$\sigma^* : A/Y \longrightarrow A/X,$$

which maps an arrow $f : C \to Y$ *in* A/Y *to that one of* A/X *by pulling* f *back along* σ, *i.e.*

$$\begin{array}{ccc} C & & \sigma^*(f) \xrightarrow{\pi_2} C \\ {\scriptstyle f}\downarrow & \longmapsto & \downarrow{\scriptstyle \pi_1} \quad \lrcorner \quad \downarrow{\scriptstyle f} \\ Y & & X \xrightarrow[\sigma]{} Y \end{array},$$

is monadic.

Remark 5.0.7. Let us spell out what exactly the monadicity here means. We know that the base change functor σ^* is the right adjoint to $\Sigma_\sigma := \sigma \circ -$. Thus,

$$A/X \underset{\sigma^*}{\overset{\Sigma_\sigma := \sigma \circ -}{\underset{\curvearrowleft}{\overset{\curvearrowright}{\perp}}}} A/Y \ .$$

Therefore the endofunctor $\sigma^* \circ \Sigma_\sigma : A/X \longrightarrow A/X$ is given as,

$$(D, g : D \to X) \longmapsto (X \times_Y C, \sigma^*(\sigma \circ g)) .$$

We then have the following monad on A/X,

$$\mathbb{T} = (\sigma^* \circ \Sigma_\sigma, \eta, \sigma^* \epsilon \Sigma_\sigma) .$$

Hence, the fact that σ is an effective descent morphism would mean that the following functor is an isomorphism

$$\begin{aligned} K : A/Y &\longrightarrow (A/X)^{\mathbb{T}} \\ (C, f) &\longmapsto (\sigma^*(f), \sigma^* \epsilon_f) . \end{aligned}$$

Alternatively, Beck's theorem (Theorem 12) says that $\sigma : X \to Y$ is an effective descent morphism if and only if the functor $\sigma^* : A/Y \longrightarrow A/X$ creates coequalizers for split forks in it's image.

We next come closer to defining the phenomenon of an object in a category being "split by an extension", this will get us closer to defining the analogue of a "Galois extension" in this context:

Definition 5.0.8. (**Admissible Slice Object Split by an Admissible Morphism**) *Let the following be a given relatively admissible adjunction where $\boldsymbol{C}$ has pullbacks:*

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} (A_{\mathbf{D}}, \mathbf{D}) .$$

Let C be some object of $\boldsymbol{C}$. We then say that an object $(X, f : X \to C) \in A_{\mathbf{C}}/C$ is split by a morphism $\sigma : S \to C$ in $A_{\mathbf{C}}$ if the unit $\tilde{\eta} : 1_{\mathbf{C}/S} \Longrightarrow \eta_S^* R(-) \circ L|_{\mathbf{C}/S}$ of the restricted adjunction derived from Lemma 5.0.1 as below

$$A_{\mathbf{C}}/S \subseteq \mathbf{C}/S \underset{\eta_S^* R(-)}{\overset{L|_{\mathbf{C}/S}}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} \mathbf{D}/LS \supseteq A_{\mathbf{D}}/LS ,$$

takes the image of $\sigma^* : A_{\mathbf{C}}/C \longrightarrow A_{\mathbf{C}}/S$ for the object (X, f), $\sigma^*(X, f)$, such that the unit component at $\sigma^*(X, f)$

$$\tilde{\eta}_{\sigma^*(X,f)} : \sigma^*(X, f) \longrightarrow \eta_S^* R\,(LX, Lf)$$

is an isomorphism.

Remark 5.0.9. Definition 5.0.8 can be written down as demanding the dashed arrow below to be an isomorphism:

$$\begin{array}{ccccccc} X & \longleftarrow & S \times_C X & \overset{\tilde{\eta}_{\sigma^*(X,f)}}{\overset{\cong}{\dashrightarrow}} & P & \longrightarrow & RL(S \times_C X) \\ {\scriptstyle f \in A_{\mathbf{C}}}\downarrow & \lrcorner & \downarrow{\scriptstyle \sigma^*(X,f)} & & \downarrow{\scriptstyle \eta_S^*(RL\sigma^*(X,f))} & & \downarrow{\scriptstyle RL\sigma^*(X,f)} \\ C & \underset{\sigma \in A_{\mathbf{C}}}{\longleftarrow} & S & = & S & \underset{\eta_S}{\longrightarrow} & RLS \end{array} .$$

We finally define relative Galois descent:

Definition 5.0.10. (**Relative Galois Descent**) *Let the following be a given relatively admissible adjunction where both* $\boldsymbol{C}$ *and* $\boldsymbol{D}$ *have pullbacks:*

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\rightleftarrows}} (A_{\mathbf{D}}, \mathbf{D}) \ .$$

Consider a morphism $\sigma : S \to C$ *in* $\boldsymbol{C}$*. We define* σ *to be a relative Galois descent with respect to* $R \vdash L$ *if the following conditions are satisfied:*

1. *The morphism* $\sigma : S \to C$ *is an effective descent morphism relative to* $A_{\mathbf{C}}$*.*
2. *The counit of the adjunction*

$$\mathbf{C}/S \underset{\eta_S^* R(-)}{\overset{L|_{\mathbf{C}/S}}{\rightleftarrows}} \mathbf{D}/LS \ ,$$

   denoted by

$$\tilde{\epsilon} : L|_{\mathbf{C}/C} \circ \eta_C^* R(-) \Longrightarrow 1_{\mathbf{D}/LS},$$

   is an isomorphism.

3. *Take any object* (Y, g) *in the admissible slice* $A_{\mathbf{D}}/LS \subseteq \boldsymbol{D}/LS$*. The object*

$$\Sigma_\sigma \circ \eta_S^* R(Y, g) = \sigma \circ \eta_S^* Rg \in A_{\mathbf{C}}/C$$

   is split by $\sigma : S \to C$*.*

Remark 5.0.11. The 3rd axiom of the above definition needs some explaining to do, which we do now. First note the following diagram:

$$\begin{array}{ccc} \eta_S^* Rg & \xrightarrow{\pi_2} & RY \\ {\scriptstyle \pi_1}\downarrow & \lrcorner & \downarrow{\scriptstyle Rg} \\ S & \xrightarrow[\eta_S]{} & RLS \\ {\scriptstyle \sigma}\downarrow & & \\ C & & \end{array} \ .$$

Clearly, the 3rd axiom is demanding that the vertical composite $\sigma \circ \pi_1$ be split by the effective descent morphism $\sigma : S \to C$. Note that to be split by σ, the object $(\eta_S^* Rg, \sigma \circ \pi_1)$ must be present in $A_{\mathbf{C}}/C$ (Definition 5.0.8). This follows from the fact that $R \vdash L$ is a relatively admissible adjunction so that the admissible slice $g : Y \to LS$ in $\mathbf{D}$ is taken to an admissible slice $Rg : RY \to RLS$ in $\mathbf{C}$. Moreover, η_S is admissible in $\mathbf{C}$, and thus the pullback π_1 is admissible. Hence, $\sigma \circ \pi_1$ is admissible and thus σ can indeed split $\sigma \circ \pi_1$.

Remark 5.0.12. (**Notation Change**) The above definitions used notation which helped in explicitly stating the role of the functors in hand. However, the above notation would not help in clearly stating complicated results about them. We thus make the following notation change:

$$L_S := L|_{\mathbf{C}/S} : A_{\mathbf{C}}/S \rightleftarrows A_{\mathbf{D}}/LS : \eta_S^* R(-) =: R_S.$$

The counit-unit pair of $R_S \vdash L_S$ would now be denoted as ϵ^S-η^S, which was previously denoted as $\tilde{\epsilon}$-$\tilde{\eta}$.

Remark 5.0.13. (**All adjunctions so far**) To get a complete view of the situation we are setting (in particular, of Definition 5.0.10), here are all the adjunctions so far. Let $\sigma : S \to C$ be an arrow in $\mathbf{C}$:

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} (A_{\mathbf{D}}, \mathbf{D})$$

$$\begin{array}{ccc} A_{\mathbf{C}}/S & \underset{\sigma^*}{\overset{\Sigma_\sigma}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} & A_{\mathbf{C}}/C \\ R_S \vdash L_S \uparrow\downarrow & & \uparrow\downarrow L_C \dashv R_C \\ A_{\mathbf{D}}/LS & \underset{(L\sigma)^*}{\overset{\Sigma_{L\sigma}}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} & A_{\mathbf{D}}/LC \end{array} \qquad S \xrightarrow{\ \sigma\ } C .$$

We then have following points to note:

- Definition 5.0.8 demands the unit of left column of the above square, $R_S \vdash L_S$, to have isomorphic component at the object $\sigma^*(X, f)$ in order to call $(X, f) : X \to C$ in $A_{\mathbf{C}}$ be an object split by some $\sigma : S \to C$ in $A_{\mathbf{C}}$.
- Definition 5.0.10 demands the left row of the above square, $R_S \vdash L_S$, to have an isomorphic counit and the arrow $\sigma \circ R_S(g) : \eta_S^* Rg \to C$ to be split by the effective descent morphism $\sigma : S \to C$ in order to call σ a relative Galois descent.

With this, we have set up the definitions that will be used in deriving some lemmas before proving the main theorem. Regarding examples of the above terminology, I think it would be best if we first prove the general Galois theorem, and then as it's example, we show the Galois theory over commutative rings, and then show that it contains all the theories we have studied upto now.

5.1 Preliminary results

We now prove some quick lemmas, most of which follows directly by unraveling of the definitions introduced above. This also provides a good place to understand above definitions a bit deeper.

Main goal of this subsection : To state and prove results prior to categorical Galois theorem.

Lemma 5.1.1. Let the following be a relatively admissible adjunction where both $\mathbf{C}$ and $\mathbf{D}$ have pullbacks:

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\underset{\curvearrowleft}{\overset{\curvearrowright}{\bot}}}} (A_{\mathbf{D}}, \mathbf{D})$$

and let the following be the slice adjunctions induced by above at objects S and C of $\mathbf{C}$:

$$A_{\mathbf{C}}/S \subseteq \mathbf{C}/S \underset{R_S}{\overset{L_S}{\underset{\curvearrowleft}{\overset{\curvearrowright}{\bot}}}} \mathbf{D}/LS \supseteq A_{\mathbf{D}}/LS \qquad A_{\mathbf{C}}/C \subseteq \mathbf{C}/C \underset{R_C}{\overset{L_C}{\underset{\curvearrowleft}{\overset{\curvearrowright}{\bot}}}} \mathbf{D}/LC \supseteq A_{\mathbf{D}}/LC \ .$$

Let $\sigma : S \to C$ in $\mathbf{C}$ be a relative Galois descent with respect to $R \vdash L$. Then the following are two equalities:

1. $\Sigma_{L\sigma} \circ L_S = L_C \circ \Sigma_\sigma$.
2. $R_S \circ (L\sigma)^* = \sigma^* \circ R_C$.

Proof. Take any $f : X \to S$ in $A_{\mathbf{C}}/S$. We then have

$$\Sigma_{L\sigma} \circ L|_{\mathbf{C}/S}(f) = L\sigma \circ Lf = L(\sigma \circ f)$$

and

$$L|_{\mathbf{C}/C} \circ \Sigma_\sigma(f) = L(\sigma \circ f),$$

thus establishing the first result. Next, take any $g : Y \to LC$ in $A_{\mathbf{D}}/LC$. We then have the following two diagrams which explains the rest:

$$\begin{array}{ccccc} Q & \longrightarrow & RP & \longrightarrow & RY \\ {\scriptstyle\pi}\downarrow & \lrcorner & \downarrow & \lrcorner & \downarrow{\scriptstyle Rg} \\ S & \xrightarrow[\eta_S]{} & RLS & \xrightarrow[RL\sigma]{} & RLC \end{array} \qquad \begin{array}{ccccc} B & \longrightarrow & A & \longrightarrow & RY \\ {\scriptstyle p}\downarrow & \lrcorner & \downarrow & \lrcorner & \downarrow{\scriptstyle Rg} \\ S & \xrightarrow[\sigma]{} & C & \xrightarrow[\eta_C]{} & RLC \end{array}$$

where $\eta_C \circ \sigma = RL\sigma \circ \eta_S$ because the RHS is the adjoint transpose of $L\sigma$ and adjoint transpose of LHS can be seen (with few more diagrams typical of adjunctions) to be equal to $L\sigma$. Thus the pullbacks p and π are same. ■

5.1.1 Three foundational lemmas

We discuss three lemmas which will be ubiquitous in what follows. The following result answers the question : **when is an admissible arrow split by identity?**

Lemma 5.1.2. Let the following be a relatively admissible adjunction where both $\mathbf{C}$ and $\mathbf{D}$ have pullbacks:

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\rightleftarrows}} (A_{\mathbf{D}}, \mathbf{D}) \quad (\perp)$$

and let the following be the slice adjunctions induced by above at object S of $\mathbf{C}$:

$$A_{\mathbf{C}}/S \subseteq \mathbf{C}/S \underset{R_S}{\overset{L_S}{\rightleftarrows}} \mathbf{D}/LS \supseteq A_{\mathbf{D}}/LS \ . \quad (\perp)$$

Let $(X, f : X \to S)$ be an object in $A_{\mathbf{C}}/S$. Then the following are equivalent:

1. (X, f) is split by $1_S : S \to S$.
2. The unit η^S of $R_S \vdash L_S$ at (X, f) is an isomorphism. That is, the following arrow

   $$\eta^S_{(X,f)} : (X, f) \longrightarrow R_S L_S (X, f)$$

   is an isomorphism in $A_{\mathbf{C}}/S$.
3. $(X, f) \cong R_S(Y, g)$ for some $(Y, g : Y \to LS)$ in $A_{\mathbf{D}}/LS$.

Proof. (1 $\implies$ 2) Since (X, f) is split by $1_S : S \to S$, thus by Definition 5.0.8, $\eta^S_{1^*_S(X,f)}$ is an isomorphism. But $1^*_S(X, f)$ is isomorphic to (X, f) because pullback along identity gives you the same arrow which you began with. Hence $\eta^S_{(X,f)}$ is an isomorphism, which is what statement 2 is.
(2 $\implies$ 1) Again, since $1^*_S(X, f) \cong (X, f)$ and since $\eta^S_{(X,f)}$ is an isomorphism, thus $\eta^S_{1^*_S(X,f)}$ is an isomorphism. The latter thus means that 1_S splits (X, f).
(2 $\implies$ 3) Trivially, let $(Y, g) = L_S(X, f)$, then $\eta^S_{(X,f)}$ establishes the required isomorphism between (X, f) and $R_S(Y, g)$.
(3 $\implies$ 1) Since $\sigma : S \to C$ is a relative Galois descent, thus by Definition 5.0.10, 2, we have that counit ϵ^S of $R^S \vdash L^S$ is an isomorphism. This gives us the following chain of isomorphism:

$$(X, f) \cong R_S(Y, g) \cong R_S\left(L_S R_S(Y, g)\right) \cong R_S L_S(X, f).$$

Then, by drawing adjoint triangle for the above isomorphism, we can see that $\eta^S_{(X,f)}$ is indeed an isomorphism. ■

And the next result characterizes **when is an admissible slice object split by a relative Galois descent**, thus the following is an important lemma:

Lemma 5.1.3. Let the following be a relatively admissible adjunction where both $\mathbf{C}$ and $\mathbf{D}$ have pullbacks:

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} (A_{\mathbf{D}}, \mathbf{D})$$

and let the following be the slice adjunctions induced by above at objects S and C of $\mathbf{C}$:

$$A_{\mathbf{C}}/S \subseteq \mathbf{C}/S \underset{R_S}{\overset{L_S}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} \mathbf{D}/LS \supseteq A_{\mathbf{D}}/LS \qquad A_{\mathbf{C}}/C \subseteq \mathbf{C}/C \underset{R_C}{\overset{L_C}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} \mathbf{D}/LC \supseteq A_{\mathbf{D}}/LC \ .$$

Let $(X, f : X \to C)$ be an object of $A_{\mathbf{C}}/C$. Let $\sigma : S \to C$ be a relative Galois descent with respect to $R \vdash L$. Then, the following are equivalent:

1. (X, f) is split by $\sigma : S \to C$.
2. $\sigma^*(X, f)$ is split by $1_S : S \to S$.
3. $\sigma^*(X, f) \cong R_S(Y, g)$ for some $(Y, g : Y \to LS)$ in $A_{\mathbf{D}}/LS$.

Proof. (1 $\implies$ 2) Given that $\eta^S_{\sigma^*(X,f)} : \sigma^*(X, f) \longrightarrow R_S L_S(\sigma^*(X, f))$ is an isomorphism, since the pullback of any arrow $\bullet \to S$ along 1_S would be the same arrow back, hence $1^*_S\left(\sigma^*(X, f)\right) \cong \sigma^*(X, f)$. Thus, $\eta^S_{1^*_S(\sigma^*(X,f))} \cong \eta^S_{\sigma^*(X,f)}$ and we know that the latter is an isomorphism.
(2 $\implies$ 1) Again, we are given that $\eta^S_{1^*_S(\sigma^*(X,f))}$ is an isomorphism, but $\eta^S_{1^*_S(\sigma^*(X,f))} \cong \eta^S_{\sigma^*(X,f)}$, hence $\sigma : S \to C$ splits (X, f).
(2 $\implies$ 3) By Lemma 5.1.2, 2, the fact that $1_S : S \to S$ splits $\sigma^*(X, f)$ gives the isomorphism $\sigma^*(X, f) \cong R_S L_S \sigma^*(X, f)$, so simply let $(Y, g) = L_S \sigma^*(X, f)$.
(3 $\implies$ 2) Simply use Lemma 5.1.2, 1. ■

Remark 5.1.4. What we saw in Lemmas 5.1.2 and 5.1.3 is that the subcategory of all objects of $A_{\mathbf{C}}/S$ which are split by a morphism 1_S are given by, upto isomorphism, an image of R_S for some object in $A_{\mathbf{D}}/LS$. A natural question arises: **is every object of $A_{\mathbf{D}}/LS$ obtained by those objects of $A_{\mathbf{C}}/S$ split by** 1_S? The answer is yes and the following lemma is the witness.

Lemma 5.1.5. Let the following be a relatively admissible adjunction where both $\mathbf{C}$ and $\mathbf{D}$ have pullbacks:

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\rightleftarrows}} (A_{\mathbf{D}}, \mathbf{D}) \ .$$

Denote $\mathbf{Split}_S(1_S)$ to be the subcategory of $A_{\mathbf{C}}/S$ which are split by $1_S : S \to S$. Then the following restricted adjunction

$$\mathbf{Split}_S(1_S) \subseteq A_{\mathbf{C}}/S \subseteq \mathbf{C}/S \underset{R_S}{\overset{L_S}{\rightleftarrows}} \mathbf{D}/LS \supseteq A_{\mathbf{D}}/LS$$

establishes an equivalence of categories. That is,

$$\mathbf{Split}_S(1_S) \equiv A_{\mathbf{D}}/LS.$$

Proof. The fact that this establishes isomorphism in homsets is trivial. Take any object $(X, f : X \to S)$ in $\mathbf{Split}_S(S)$, so that $1_S : S \to S$ splits $f : X \to S$. Now, by Lemma 5.1.2, 3, there exists $(Y, g : Y \to LS)$ in $A_{\mathbf{D}}/LS$ such that $(X, f) \cong R_S(Y, g)$. Hence, R_S is essentially surjective. This proves the result. ■

The Lemmas 5.1.2, 5.1.3 & 5.1.5 are important and will be used frequently, especially the Lemmas 5.1.2 and 5.1.3 as they can be used to translate a question about an object being split by a relative Galois descent to a question of some other object being split by the identity.
Let us now study a bit of internal category theory, in preparation for the abstract Galois theorem. Most of what follows is elementary and quite intuitive.

5.1.2 Internal categories & internal presheaves

Internalization is the process of interpreting the axioms of a given mathematical structure in the internal language of a category with enough structure. It is quite powerful of a tool for generalization, because a theorem proved for, say general group object in any ambient category will hold for usual groups (in **Grp**), topological groups (in **Top**), Lie groups (in **Diff**), etc. Even then, one can go on interpret a given first order signature inside a category and then internally to that category, instantiate terms, formulas, theories and models; this is the beginning of categorical semantics, whose effect is akin to changing the meta-language of first order logic.
However, one can go further. What about internalizing the axioms of a category inside another category (with enough structure, of-course)? The result is an internal category, the definition of which, like most internalized definitions, is quite diagrammatic[32].

Definition 5.1.6. (**Internal Category**) Let $\mathbf{A}$ be a category with all pullbacks. We say that the pair of objects (C_0, C_1) of $\mathbf{A}$ defines an internal category with C_0 and C_1 being the object of objects and object of arrows respectively, if there are the following arrows in $\mathbf{C}$

- ***Source & target morphisms*** given by

$$s, t : C_1 \rightrightarrows C_0$$

[32]note that we will give very *loose* definitions and no proofs as we don't wish to be bogged down by very minute details. For more details, refer to Chapter 8 of [Bor94].

- ***Identity assignment morphism*** given by

$$e : C_0 \to C_1$$

- ***Composition morphism*** given by $c : C_1 \times_{C_0} C_1 \to C_1$ which is the pullback of s along t

$$\begin{array}{ccc} C_1 \times_{C_0} C_1 & \xrightarrow{c} & C_1 \\ \downarrow & \lrcorner & \downarrow{\scriptstyle t} \\ C_1 & \xrightarrow[s]{} & C_0 \end{array}$$

subjected to the conditions which in words says that

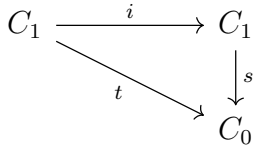
1. The composition morphism is well defined[33].
2. The identity arrow for each object is left and right unital.
3. Composition is associative.

Obviously, Definition 5.1.6 is not a complete definition; the complete definition would include a lot of diagrams representing each of the conditions mentioned above, but such an explicit description would rarely be useful. We similarly define the notion of an internal groupoid:

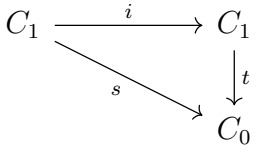
Definition 5.1.7. (**Internal Groupoid**) Let **A** be a category with all pullbacks. An internal category (C_0, C_1, s, t, e, c) in **A** is said to be an internal groupoid if there is additionally an arrow

$$i : C_1 \longrightarrow C_1$$

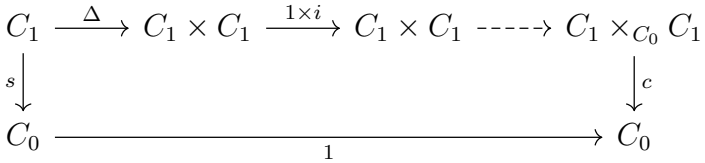
such that all of the following diagram commutes:



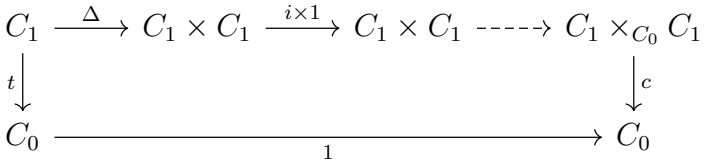
source of f^{-1} is target of f



target of f^{-1} is source of f



$f^{-1} \circ f = 1_{s(f)}$



$f \circ f^{-1} = 1_{t(f)}$

We next (tersely!) define the notion of an internal covariant presheaf:

[33] meaning that it takes composable pair of "arrows" (in C_1) to an "arrow" whose source is source of one of them and target is the target of the other.

Definition 5.1.8. (**Internal Covariant Presheaf**) Let $\mathbf{A}$ be a category with all pullbacks and let (C_0, C_1, s, t, e, c) be an internal category in $\mathbf{A}$. An internal covariant presheaf over internal category (C_0, C_1) is a triple (P, p, π) where P is an object of $\mathbf{A}$, $p : P \longrightarrow C_0$ is an arrow in $\mathbf{A}$ and $\pi : C_1 \times_{C_0} P \longrightarrow P$ as in

$$\begin{array}{ccc} C_1 \times_{C_0} P & \xrightarrow{\alpha_2} & P \\ {\scriptstyle \alpha_1}\downarrow & \lrcorner & \downarrow{\scriptstyle p} \\ C_1 & \xrightarrow[s]{} & C_0 \end{array}$$

such that the following square commutes

$$\begin{array}{ccc} C_1 \times_{C_0} P & \xrightarrow{\pi} & P \\ {\scriptstyle \alpha_1}\downarrow & & \downarrow{\scriptstyle p} \\ C_1 & \xrightarrow[t]{} & C_0 \end{array} .$$

We also require (P, p, π) to respect identities and composition, but we don't draw those diagrams here.

Note that the above definition simply defines P to be the disjoint union of all sections of presheaf P and the other commutative diagram simply tell us how this presheaf behaves under arrows, as one might guess from letting the ambient category $\mathbf{A}$ to be the category of sets.
The next step would be to (tersely!!) define an internal natural transformation between internal covariant presheaves:

Definition 5.1.9. (**Internal Natural Transformation**) Let $\mathbf{A}$ be a category with pullbacks and let (P, p, π) and (P', p', π') be two internal covariant presheaves. A natural transformation

$$\eta : (P, p, \pi) \longrightarrow (P', p', \pi')$$

is defined to be an arrow $\eta : P \longrightarrow P'$ of $\mathbf{A}$ such that the following commutes

$$\begin{array}{ccc} P & \xrightarrow{\eta} & P' \\ & {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle p'} & \\ & C_0 & \end{array} .$$

We also require η to follow the diagrammatic natural square, but we don't draw that diagram here.

Note that the above commutative triangle expresses the usual fact that a natural transformation of presheaves maps a section of a presheaf at some object to a section of the other presheaf but at the same object.

Remark 5.1.10. (**The internal presheaf category**) Let $\mathbf{A}$ be a category with all pullbacks. The collection of all internal covariant presheaves on an internal category $C = (C_0, C_1, s, t, e, c)$ and internal natural transformations between them constitutes a subcategory of $\mathbf{A}$, which we denote by $\mathbf{A}^C$.

The following is a result which will be used in the discussion that follows. Proof will be somewhere in *Elephant* [Joh02].

Proposition 5.1.11. Let $\mathbf{A}$ be a category with all pullbacks and let $C = (C_0, C_1)$ be an internal category in $\mathbf{A}$. Then the following functor

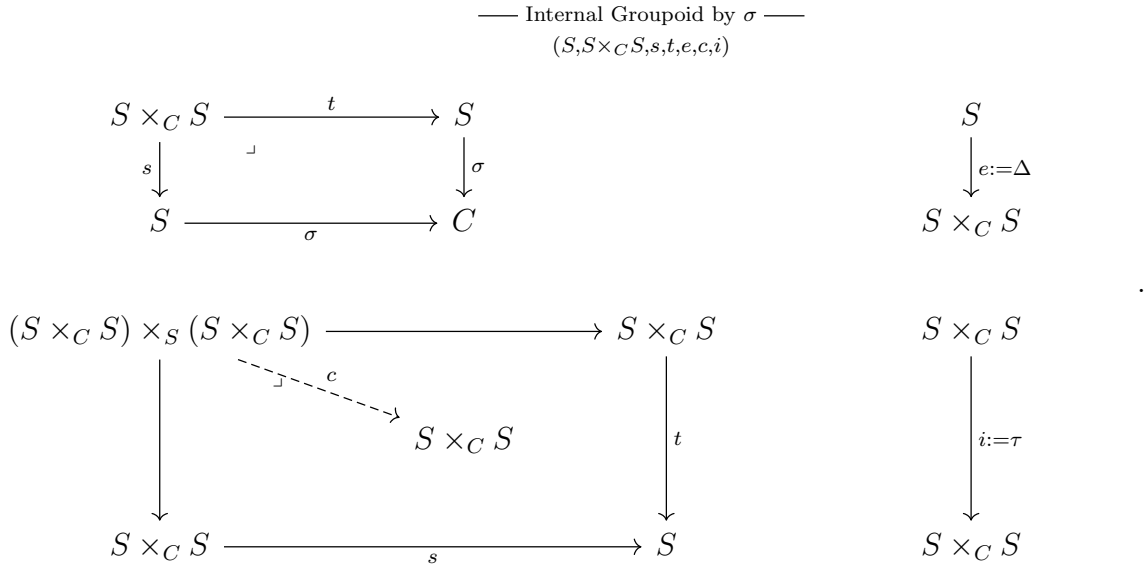
$$\begin{aligned} \mathbf{A}^C &\longrightarrow \mathbf{A}/C_0 \\ (P, p, \pi) &\longmapsto (P, p) \end{aligned}$$

is monadic.

5.1.3 Internal groupoid associated to an arrow

For every arrow in a category with pullbacks, one can attach an internal groupoid, by the following construction:

Proposition 5.1.12. Let $\mathbf{A}$ be a category with all pullbacks. Let $\sigma : S \to C$ be an arrow in $\mathbf{A}$. The data $(S, S \times_C S, s, t, e, c, i)$ where all the relevant arrows are described in the figure below, induces an internal groupoid in $\mathbf{A}$.



Proof. We need to check whether all the diagrams of Definitions 5.1.7 commutes in this case or not. First, $s \circ i = t$ and $t \circ i = s$ are both obvious in this case by definition of $s, t : S \times_C S \to S$. The other two follows easily from the diagrams in their definitions. ■

We know that any function $f : X \to Y$ in **Sets** gives an equivalence relation on the set X by fibers of f. If we define a category whose objects are elements of X and arrows given by whether they evaluate under f to the same object, then this category is actually a groupoid. Proposition 5.1.12 is the generalization of this trivial fact internal to any category with pullbacks.

5.1.4 More results

We now discuss some more lemmas, but because their proofs are very easy and requires only the hypotheses which we have dealt with in previous lemmas, therefore it will be quite nice to present them in one setting:

Theorem 13. Let the following be a relatively admissible adjunction where both $\mathbf{C}$ and $\mathbf{D}$ have pullbacks:

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} (A_{\mathbf{D}}, \mathbf{D})$$

and let the following be the slice adjunctions induced by above at objects S and C of $\mathbf{C}$:

$$A_{\mathbf{C}}/S \subseteq \mathbf{C}/S \underset{R_S}{\overset{L_S}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} \mathbf{D}/LS \supseteq A_{\mathbf{D}}/LS \qquad A_{\mathbf{C}}/C \subseteq \mathbf{C}/C \underset{R_C}{\overset{L_C}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} \mathbf{D}/LC \supseteq A_{\mathbf{D}}/LC \ .$$

We then have the following results:

1. Let $\sigma : S \to C$ be a relative Galois descent in $\mathbf{C}$. If $(X, f : X \to S) \in A_{\mathbf{C}}/S$ is split by $1_S : S \to S$, then $\sigma^* \circ \Sigma_\sigma(X, f)$ is also split by $1_S : S \to S$.

2. The object $(S, 1_S : S \to S) \in A_{\mathbf{C}}/S$ is split by $1_S : S \to S$.

3. Let $\sigma : S \to C$ be a relative Galois descent in $\mathbf{C}$. The object $(C, 1_C : C \to C)$ is split by $\sigma : S \to C$.

4. Let $\sigma : S \to C$ be a relative Galois descent in $\mathbf{C}$. For all $n \in \mathbb{N}$ and all $1 \leq i \leq n$, the objects $(\prod_{i=1}^n S, p_i) \in A_{\mathbf{C}}/S$ are all split by $1_S : S \to S$ where $p_i : \prod_{i=1}^n S \longrightarrow S$ are the projection maps in the admissible slice category $A_{\mathbf{C}}/S$.

5. If $(X_1, f_1 : X \to S)$ and $(X_2, f_2 : X \to S)$ in $A_{\mathbf{C}}/S$ are split by $1_S : S \to S$, then $(X_1, f_1) \prod (X_2, f_2) \in A_{\mathbf{C}}/S$ is also split by $1_S : S \to S$.

6. Let $\sigma : S \to C$ be a relative Galois descent in $\mathbf{C}$. Denote $\mathbf{Split}_C(\sigma)$ to be the full subcategory of $A_{\mathbf{C}}/C$ of all those objects which are split by σ. The pullback functor $\sigma^* : A_{\mathbf{C}}/C \longrightarrow A_{\mathbf{C}}/S$ restricts to the functor

$$\sigma^* : \mathbf{Split}_C(\sigma) \longrightarrow \mathbf{Split}_S(1_S)$$

which is a monadic functor.

7. Let $\sigma : S \to C$ be a relative Galois descent in $\mathbf{C}$. The functor

$$\begin{aligned} L_S \circ \sigma^*(-) : \mathbf{Split}_C(\sigma) &\longrightarrow A_{\mathbf{D}}/LS \\ (X, f : X \to C) &\longmapsto L_S \circ \sigma^*(X, f) \end{aligned}$$

is monadic.

8. Let $\sigma : S \to C$ be a relative Galois descent in $\mathbf{C}$. The internal groupoid in $\mathbf{C}$ induced by σ as in Proposition 5.1.12 is taken by left adjoint $L : \mathbf{C} \longrightarrow \mathbf{D}$ to an internal groupoid in $\mathbf{D}$.

Proof. Here are the proofs:-

1. Since $(X, f : X \to S) \in A_{\mathbf{C}}/S$ is split by $1_S : S \to S$, Lemma 5.1.2 tells us that $\exists (Y, g : Y \to LS) \in A_{\mathbf{D}}/LS$ such that $(X, f) \cong R_S(Y, g)$. Now because $\sigma : S \to C$ is a relative Galois descent, therefore by Definition 5.0.10, 3, we have that $\Sigma_\sigma \circ R_S(Y, g)$ in $A_{\mathbf{C}}/\mathbf{C}$ is split by $\sigma : S \to C$. Note that $\Sigma_\sigma \circ R_S(Y, g)$ is indeed admissible (in $A_{\mathbf{C}}$, that is) because $R_S \vdash L_S$ is relatively admissible and $\sigma : S \to C$ is a relative Galois descent and hence an effective descent morphism and hence admissible. Finally, Lemma 5.1.3, 2, tells us that $\sigma^* \circ \Sigma_\sigma \circ R_S(Y, g) \cong \sigma^* \circ \Sigma_\sigma(X, f)$ in $A_{\mathbf{C}}/\mathbf{S}$ is split by $1_S : S \to S$. This proves the result.

2. We first see that $R_S L_S(S, 1_S) = R_S(L_S S, 1_{L_S S}) = (S, 1_S)$ where the last equality follows from the observation that pullback of identity is identity. This makes $\eta^S : S \to R_S L_S S$ identity which can be seen by it's explicit description in Remark 5.0.2 (draw the diagram for utmost clarity). Lemma 5.1.2, 2, does the rest of the job.

3. Now since $(S, 1_S : S \to S) \in A_{\mathbf{C}}/S$ is such that $\sigma^*(C, 1_C) = (S, 1_S) \in A_{\mathbf{C}}/S$, therefore by Lemma 5.1.3, 1, $(C, 1_C : C \to C)$ is split by the relative Galois descent $\sigma : S \to C$

4. We will use induction on $n \in \mathbb{N}$. For $n = 1$, the object $(S, 1_S) \in A_{\mathbf{C}}/S$ is trivially split by 1_S due to result 2. Note that a finite product is a form of pullback, and hence admissible classes are also closed under finite products. Let $(\prod_{i=1}^k S, p_i) \in A_{\mathbf{C}}/S$ be split by 1_S for all $1 \leq i \leq n$. We wish to show that $(\prod_{i=1}^{k+1} S, p_i) \in A_{\mathbf{C}}/S$ is also split by 1_S for all $1 \leq i \leq n$. By 1, we must have that since $(\prod_{i=1}^k S, p_i) \in A_{\mathbf{C}}/S$

is split by 1_S, then so should $\sigma^* \circ \Sigma_\sigma \left(\prod_{i=1}^k S, p_i \right)$. Now we have the following pullback diagram, which explains the rest:

$$\begin{array}{ccc} \prod_{i=1}^{k+1} S & \longrightarrow & \prod_{i=1}^{k} S \\ {\scriptstyle p_i}\downarrow & \lrcorner & \downarrow{\scriptstyle \sigma \circ p_i} \\ S & \xrightarrow[\sigma]{} & C \end{array}.$$

Note that the above is indeed a pullback and it can be checked by taking any cone over it and seeing that there exists a unique universal map from the summit to $\prod_{i=1}^{k+1} S$. This completes the induction and hence the proof.

5. Using Lemma 5.1.2, we see that there exists $(Y_1, g_1), (Y_2, g_2) \in A_{\mathbf{C}}/LS$ such that $(X_1, f_1) \cong R_S(Y_1, g_1)$ and $(X_2, f_2) \cong R_S(Y_2, g_2)$. But since $R_S \vdash L_S$ is an adjunction and so R_S preserves limits, and hence $(X_1, f_1) \prod (X_2, f_2) \cong R_S(Y_1, g_1) \prod R_S(Y_2, g_2) \cong R_S((Y_1, g_1) \prod (Y_2, g_2))$. Now again by Lemma 5.1.2 (or by Lemma 5.1.5), we see that $(X_1, f_1) \prod (X_2, f_2)$ is split by $1_S : S \to S$.

6. Before we do anything, we need to check whether σ^* has a left adjoint or not. Obviously, we should first check whether $\Sigma_\sigma : A_{\mathbf{C}}/S \longrightarrow A_{\mathbf{C}}/C$ restricts to it's left adjoint. A trivial computation using the result no. 1 above and Lemma 5.1.3 tells us that indeed, the adjunction $\sigma^* \vdash \Sigma_\sigma$ restricts to an adjunction between $\mathbf{Split}_S(1_S)$ and $\mathbf{Split}_C(\sigma)$. Next, we need to see whether σ^* is monadic when it undergoes such restriction. For that, we first observe that σ is a relative Galois descent, so by Definition 5.0.10, $\sigma : S \to C$ is indeed an effective descent morphism, which in particular means that $\sigma^* : A_{\mathbf{C}}/C \longrightarrow A_{\mathbf{C}}/S$ is monadic. However, this doesn't necessitate σ^* to restrict to a monadic functor on split objects. So for this, we use Beck's criterion as in Theorem 12. Take any parallel pair in $\mathbf{Split}_C(\sigma)$ such that it's image under σ^* is a split fork in $\mathbf{Split}_S(1_S)$. By monadicity of the unrestricted σ^*, σ^* has created a coequalizer of the original parallel pair, but in $A_{\mathbf{C}}/C$, not in $\mathbf{Split}_C(\sigma)$. This coequalizer in $A_{\mathbf{C}}/C$ maps to the split coequalizer of the image of this parallel pair in $\mathbf{Split}_S(1_S)$. By result 1 and Lemma 5.1.3 we can see that this coequalizer in $A_{\mathbf{C}}/C$ created by σ^*, is indeed inside $\mathbf{Split}_C(\sigma)$.

7. We will use Beck's criterion (Theorem 12). Take a parallel pair in $\mathbf{Split}_C(\sigma)$ such that it's image is a split fork in $A_{\mathbf{D}}/LS$. The rest follows by observing the equivalence given by Lemma 5.1.5 which gives us a split fork in $\mathbf{Split}_S(1_S)$ and then by monadicity of $\sigma^* : \mathbf{Split}_C(\sigma) \to \mathbf{Split}_S(1_S)$ as just proved in result 6 above.

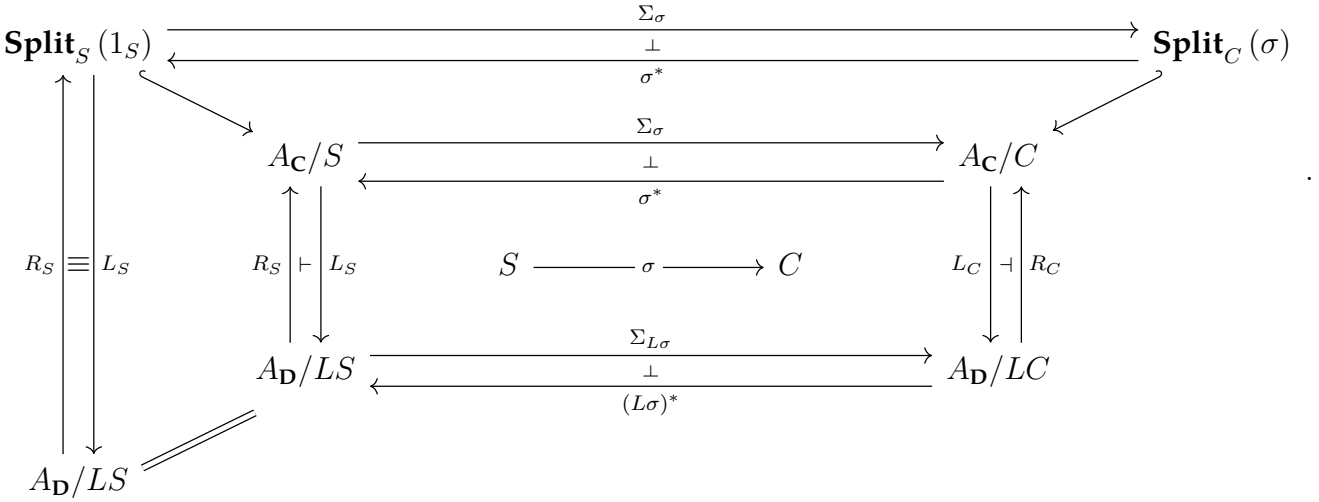
8. Omitted. ■

This theorem and the three lemmas prior to it forms the building blocks of what will follow next. Before going any further, let us make another diagram supplementing Remark 5.0.13 but now with the results obtained in Theorem 13.

Remark 5.1.13. (**The picture so far**) The picture of all the structures discovered so far is as follows

(contrast it with that of Remark 5.0.13):

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} (A_{\mathbf{D}}, \mathbf{D})$$



Note we denote $R_S \equiv L_S$ to mean that R_S and L_S adjoint and establishes an equivalence of categories.

5.2 Categorical Galois theorem

We now see the main theorem of this section, or rather this part of text, which is the Galois theorem of Janelidze. For this, we need to see that a relatively admissible adjunction preserves the internal groupoid associated to each arrow.

Lemma 5.2.1. Let the following be a relatively admissible adjunction where both $\mathbf{C}$ and $\mathbf{D}$ have pullbacks:

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} (A_{\mathbf{D}}, \mathbf{D}) \ .$$

Let $\sigma : S \to C$ be a relative Galois descent in $\mathbf{C}$. The internal groupoid associated to $\sigma : S \to C$ in $\mathbf{C}$ as in Proposition 5.1.12, is preserved by the functor L, to give an internal groupoid in $\mathbf{D}$.

Proof. Omitted. ■

We thus define the following, which names a specific internal groupoid associated to a relative Galois descent to be a Galois groupoid:

Definition 5.2.2. (**Galois Groupoid of a relative Galois Descent**) *Let the following be a relatively admissible adjunction where both $\mathbf{C}$ and $\mathbf{D}$ have pullbacks:*

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\underset{\longleftarrow}{\overset{\longrightarrow}{\bot}}}} (A_{\mathbf{D}}, \mathbf{D}) \ .$$

Let $\sigma : S \to C$ be a relative Galois descent in $\mathbf{C}$. The groupoid in $\mathbf{D}$ obtained by the image of groupoid associated to σ in $\mathbf{C}$ as in Lemma 5.2.1 is said to be the Galois groupoid $\mathbf{Gal}[\sigma]$ of the $\sigma : S \to C$.

Let us first state the main theorem and sketch it's proof before unraveling it in special case of rings:

Theorem 14. (**The Galois theorem of Janelidze**) Let the following be a relatively admissible adjunction where both $\mathbf{C}$ and $\mathbf{D}$ have all pullbacks:

$$(A_{\mathbf{C}}, \mathbf{C}) \underset{R}{\overset{L}{\rightleftarrows}} (A_{\mathbf{D}}, \mathbf{D}) \ .$$

Suppose $\sigma : S \to C$ is a relative Galois descent in $\mathbf{C}$ (Definition 5.0.10). We then have the following pair of slice adjunctions (Lemma 5.0.1 & Remark 5.0.12):

$$A_{\mathbf{C}}/S \subseteq \mathbf{C}/S \underset{R_S}{\overset{L_S}{\rightleftarrows}} \mathbf{D}/LS \supseteq A_{\mathbf{D}}/LS \qquad A_{\mathbf{C}}/C \subseteq \mathbf{C}/C \underset{R_C}{\overset{L_C}{\rightleftarrows}} \mathbf{D}/LC \supseteq A_{\mathbf{D}}/LC \ .$$

We now bring in the following three objects all constructed from σ in the previous pages:

1. The full subcategory $\mathbf{Split}_C(\sigma)$ of $A_{\mathbf{C}}/C$ of all those objects of $A_{\mathbf{C}}/C$ which are split by the relative Galois descent $\sigma : S \to C$.

2. The internal Galois groupoid $\mathbf{Gal}[\sigma]$ in $\mathbf{D}$, obtained from the relative Galois descent $\sigma : S \to C$ in $\mathbf{C}$ via the courtesy of Lemma 5.2.1.

3. The category of internal covariant presheaves $A_{\mathbf{D}}^{\mathbf{Gal}[\sigma]} \subset \mathbf{D}$ over the internal groupoid $\mathbf{Gal}[\sigma]$ in $\mathbf{D}$, where each covariant presheaf $(P, p, \pi) \in A_{\mathbf{D}}^{\mathbf{Gal}[\sigma]}$ has the arrow p in $A_{\mathbf{D}} \subset \mathbf{D}$ (Remark 5.1.10).

Then, the two categories introduced above are equivalent:

$$\boxed{\mathbf{Split}_C(\sigma) \equiv A_{\mathbf{D}}^{\mathbf{Gal}[\sigma]}.}$$

In words, the category of all those objects of $A_{\mathbf{C}}/C$ which are split by $\sigma : S \to C$ in $\mathbf{C}$ is equivalent to the category of all internal covariant presheaves (P, p, π) over the groupoid $\mathbf{Gal}[\sigma]$ in $\mathbf{D}$ with $p \in A_{\mathbf{D}}$.

Part II
Elliptic Curves & Galois Theory

6 Algebraic function fields of one variable

The concept of algebraic curves will be fundamental to our discussion and cryptographic applications that we seek. Note that a curve is just a variety whose dimension is 1 (details in next section). However, a curve is a very interesting object; the various basic algebro-geometric constructions that we will define in the next section becomes even more special and interesting when we consider varieties of dimension 1, i.e. a curve. One of these results is that *the local ring at a smooth point of a curve is actually a discrete valuation ring and smoothness arises only in this way* (Theorem 19). Moreover, we will see that an another important and basic algebro-geometric construction, the function field of a variety, becomes an algebraic function field of one variable in the case exactly when variety is some *nice* curve (Theorem 22). These and many other observations justify the independent study of this piece of algebra, called function fields, which will be our prime objective in this section. But before that, we need to set the stage with basic field theory.

We first study some easy facts about finite fields and move on to a quick discussion on function fields. We recall that for every prime p and a a natural n, there exists upto isomorphism only one finite field of order p^n. We denote this field by $\mathbb{F}_{p^n}$. It's characteristic is exactly p. The collection of all non-zero elements of $\mathbb{F}_{p^n}$ trivially forms a multiplicative group of order $p^n - 1$. Hence order of every element $\alpha \in \mathbb{F}_{p^n}$ divides $p^n - 1$. In particular, this group is cyclic and it can be seen by structure theorem. A simple argument also shows that for a prime p and natural n, the field $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ in $\mathbb{F}_p[x]$:

Lemma 6.0.1. Let p^n be a prime power. The field $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ in $\mathbb{F}_p[x]$.

Proof. Let $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$ and let $R \subseteq \overline{\mathbb{F}_p}$ be the set consisting of all roots of $x^{p^n} - x \in \mathbb{F}_p[x]$. We claim that R is the splitting field of it. First of all, indeed, R contains all of $\mathbb{F}_p$ as every element $\alpha \in \mathbb{F}_p$ must follow $\alpha^{p^n} = \alpha$. Next, we observe that the polynomial $x^{p^n} - x$ in $\mathbb{F}_p[x]$ has no repeating roots, because by Proposition 1.3.3, we check that the derivative of $x^{p^n} - x$ is $p^n x^{p^n - 1} - 1 = 0 - 1 = -1$ where the last equation follows from the fact that $\mathbb{F}_p$ is of characteristic p. This shows that R has p^n elements. By binomial theorem, one can assert that R is not just a set but a field. Finally, the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$ must be the smallest field extension of $\mathbb{F}_p$ containing all roots of it and R is precisely smallest such. ∎

Recall that a finite field is also called a Galois field. The reason for such name will become clear soon, when we will observe that actions of the Galois group $\textbf{Gal}\,[\mathbb{F}_{p^n} : \mathbb{F}_p]$ dictates a lot of properties of algebraic curves over finite field. So let us now study this particular Galois group for preparation for that topic.

Proposition 6.0.2. Let p be a prime and $n \in \mathbb{N}$. The Galois group $\textbf{Gal}\,[\mathbb{F}_{p^n} : \mathbb{F}_p]$ is the cyclic group of order n generated by $\alpha \mapsto \alpha^p$.

$$\textbf{Gal}\,[\mathbb{F}_{p^n} : \mathbb{F}_p] \cong \mathbb{Z}/n\mathbb{Z}.$$

Proof. The mapping $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ as $\alpha \mapsto \alpha^p$ is an automorphism of $\mathbb{F}_{p^n}$ fixing $\mathbb{F}_p$ because for all $\alpha \in \mathbb{F}_p$, $\alpha^{p-1} = 1$. It is an automorphism because of same reasons discussed in previous lemma, in particular, use binomial theorem and see that intermediate terms all become zero. Next, we wish to show that φ generates the whole Galois group. For this, take the smallest $m \in \mathbb{N}$ such that $\varphi^m = \mathrm{id}_{\mathbb{F}_{p^n}}$. Hence $\forall \alpha \in \mathbb{F}_{p^n}$, $\varphi^m(\alpha) = \alpha^{p^m} = \alpha$. Thus, every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^m} - x \in \mathbb{F}_{p^n}[x]$. This means that, in combination with the fundamental theorem of classical Galois theory (Theorem 3), $p^m \geq p^n \implies m \geq n$ and then $m \geq n = \dim[\mathbb{F}_{p^n} : \mathbb{F}_p] = |\textbf{Gal}\,[\mathbb{F}_{p^n} : \mathbb{F}_p]|$, i.e. $|\textbf{Gal}\,[\mathbb{F}_{p^n} : \mathbb{F}_p]| \leq m$. But $\varphi^m = \mathrm{id}_{\mathbb{F}_{p^n}}$ is the first m at which this happens, therefore $m \leq |\textbf{Gal}\,[\mathbb{F}_{p^n} : \mathbb{F}_p]|$. Both the inequalities then conclude that $n = |\textbf{Gal}\,[\mathbb{F}_{p^n} : \mathbb{F}_p]| = m$. This shows that φ has order n equaling the size of the Galois group, hence generating it and making it cyclic. ∎

Comments on Proof Technique. Note that in the proof, we somehow tried to form an algebraic identity satisfied by each of the member of $\mathbb{F}_{p^n}$, and then formed the corresponding polynomial and argued about it's amount of roots. Moreover, we tried to think of an identity which involved the given datum m. This is a general trick that one can employ to prove such simple results, by considering the given data and making a polynomial in that finite field which involves directly the size of the field itself, and then studying that polynomial.

The following has exactly the same proof as above

Lemma 6.0.3. Let q be a prime power. Then,

$$\mathbf{Gal}\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right] \cong \mathbb{Z}/n\mathbb{Z}$$

with generator the map $\sigma \mapsto \sigma^q$. ■

We also observe the following characterization of subfields of a finite field using Galois theory of fields and uniqueness of finite fields:

Lemma 6.0.4. Let p^m and p^n be two prime powers. The finite field $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if $m|n$.

Proof. (L $\implies$ R) Let $\mathbb{F}_{p^m}$ be a subfield of $\mathbb{F}_{p^n}$. Since $\dim[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \times \dim[\mathbb{F}_{p^m} : \mathbb{F}_p] = \dim[\mathbb{F}_{p^n} : \mathbb{F}_p]$, we thus get that $\dim[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$, hence $m|n$.
(R $\implies$ L) If $n = km$ for some $k \in \mathbb{N}$, then since $\mathbf{Gal}\left[\mathbb{F}_{p^n} : \mathbb{F}_p\right]$ is cyclic of order n, therefore by the basic fact that every factor of the order of a cyclic group determines a unique subgroup, we get that $\mathbf{Gal}\left[\mathbb{F}_{p^n} : \mathbb{F}_p\right]$ has a subgroup H of order k. Now, $\mathbf{Fix}\left(H\right)$ is an intermediate field extension of $\mathbb{F}_p$, and since by fundamental theorem (Theorem 3) $\mathbf{Gal}\left[\mathbb{F}_{p^n} : \mathbf{Fix}\left(H\right)\right] = H$, which in particular means that $|\mathbf{Gal}\left[\mathbb{F}_{p^n} : \mathbf{Fix}\left(H\right)\right]| = \dim[\mathbb{F}_{p^n} : \mathbf{Fix}\left(H\right)] = |H| = k$, hence $\dim[\mathbf{Fix}\left(H\right) : \mathbb{F}_p] = m$ and hence by uniqueness of finite fields $\mathbf{Fix}\left(H\right)$ must be $\mathbb{F}_{p^m}$. ■

In-fact, the same is true for q being any prime power.

Lemma 6.0.5. Let $q = p^k$ be some prime power. The finite field $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$ if and only if $m|n$

Proof. Follows from Lemma 6.0.4. ■

6.1 Absolute Galois group of finite fields

Main goal of this section : *To characterize the absolute Galois group of $\mathbb{F}_q$, Theorem 15.*

Notice that a finite field $\mathbb{F}_q$ for q being some prime power is a perfect field, as we show below:

Lemma 6.1.1. The finite field $\mathbb{F}_{p^n}$ is a perfect field.

Proof. The plan is as usual, we will take an algebraic extension $[K : \mathbb{F}_q]$, where $q = p^m$, and we will show that it is indeed a separable extension. Take any $k \in K$, there exists the minimal polynomial $f(x) \in \mathbb{F}_q[x]$ of k. Denote $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. We wish to show that $f(x)$ has all simple roots in $\mathbb{F}_q$. We will use Proposition 1.3.3 to this end. Since $f(k) = 0$, let us assume to the contrary that $f'(k) = 0$ too. We wish to find a contradiction. $f'(x)$ is one degree lower than $f(x)$ with $f'(k) = 0$, hence by minimality of $f(x)$, we must have that $f'(x) = 0$. Note that this doesn't mean that $f(x)$ is a constant polynomial because we are working in a field of characteristic p. We thus have $na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 = 0$, which simply means that each coefficient $na_n, (n-1)a_{n-1}, \ldots, a_1 = 0$. Now, since $a_n \neq 0$, hence $p|n$. Since $p|n$, so p does not divide $n-1$, so $a_{n-1} = 0$. In-fact, if we denote $n = dp$,

then everything except $a_{dp}, a_{(d-1)p}, a_{(d-2)p}, \ldots, a_{2p}, a_p$ is zero. We thus have that $f'(x) = a_{dp}x^{dp} + \ldots a_p x^p$, and in particular $a_{dp}k^{dp} + \ldots a_p k^p = 0$, which implies that $k^p \cdot (a_{dp}k^{(d-1)p} + \ldots a_p) = 0$, which further implies that $a_{dp}k^{(d-1)p} + \ldots a_p = 0$. This gives us another polynomial $g(x) = a_{dp}x^{(d-1)p} + \ldots a_p$ such that $g(k) = 0$. Again by minimality of $f(x)$, $g(x) = 0$ as $\deg g(x) < \deg f(x)$. Therefore $a_{dp}, \ldots a_p$ are also zero, giving us that $f(x) = 0$, which clearly is a contradiction to the fact that $f(x)$ is the minimal polynomial of $k \neq 0$ in K. ■

We needed this above discussion because we will now calculate the absolute Galois group of a finite field, that is, the Galois group of extension $[\overline{\mathbb{F}_q} : \mathbb{F}_q]$ where $\overline{\mathbb{F}_q}$ is the algebraic closure (and hence separable closure too by above lemma) of $\mathbb{F}_q$. The main theorem which we want to prove is that this absolute Galois group is equivalently given by projective limit of finite Galois groups $[\mathbb{F}_{q^i} : \mathbb{F}_q]$ for $i \in \mathbb{N}$, hence becoming a profinite group.

Let us first notice that both $\mathbb{F}_{p^n}$ and $\mathbb{F}_p$ have same algebraic closure because by Lemma 6.0.1, $\mathbb{F}_{p^n}$ is the field formed by collecting all roots of $x^{p^n} - x$ from $\overline{\mathbb{F}_p}$ and because $[\overline{\mathbb{F}_p} : \mathbb{F}_{p^n}]$ is an algebraic extension, and that is because $[\overline{\mathbb{F}_p} : \mathbb{F}_p]$ is trivially algebraic.

Let us now see what exactly is the algebraic closure of $\mathbb{F}_{p^n}$:

Proposition 6.1.2. Let q be a prime power. The algebraic closure of $\mathbb{F}_q$ is given by

$$\overline{\mathbb{F}_q} = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}.$$

Proof. Take a polynomial $f(x) = \sum_{n=0}^{m} a_n x^n$ where $a_n \in \bigcup_{i=1}^{\infty} \mathbb{F}_{q^i}$ for each n. We wish to show that $f(x)$ has all roots in $\bigcup_{i=1}^{\infty} \mathbb{F}_{q^i}$. For this, let α be a root of $f(x)$. Now note that $\exists k \in \mathbb{N}$ such that $a_n \in \mathbb{F}_{q^k}$ for all n. This follows from the following observation: let $\mathbb{F}_{q^{k_i}}$ be the smallest field in which a_i is contained, then if we set $k = \prod_{i=0}^{m} k_i$, then we observe by Lemma 6.0.5 that $\mathbb{F}_{q^{k_i}}$ is a subfield of $\mathbb{F}_{q^k}$ for all i. Now, we finally have to show that $\alpha \in \bigcup_{i=1}^{\infty} \mathbb{F}_{q^i}$. For this, we first observe that the field extension $\mathbb{F}_{q^k}(\alpha)$ is the smallest field containing the root α. But is it a finite field? For that, we first observe that $\mathbb{F}_{q^k}(\alpha)$ is a vector space over $\mathbb{F}_{q^k}$. If we can show that it is finite dimensional then we would be done. Now because $f(\alpha) = \sum_{n=0}^{m} a_n \alpha^n = 0$ in $\mathbb{F}_{q^m}(\alpha)$, then we can write it as $\alpha^m = -\sum_{n=0}^{m-1} a_m^{-1} a_n \alpha^n$. This tells us that any member of $\mathbb{F}_{q^k}(\alpha)$ can be written in terms of atmost $m-1$ power of α, hence making $\mathbb{F}_{q^k}(\alpha)$ a finite dimensional vector space over $\mathbb{F}_{q^k}$. In-fact, $\mathbb{F}_{q^k}(\alpha)$ would have $(q^k)^m$ elements, making it a finite field. ■

Remember the topics of Section 3.1, where we discussed (co)filtered systems in a category. We discussed it there in order to find a description of profinite *spaces*. We will use the same here to discuss profinite *groups*.

Definition 6.1.3. (**Profinite Groups**) Let $\mathbf{J}$ be a cofiltered poset, treated as a category. A group G in **Grp** is called profinite if there exists a cofiltered poset $\mathbf{J}$ and a functor/diagram $D : \mathbf{J} \longrightarrow \mathbf{Grp}^{\mathrm{Fin}}$ such that

$$G \cong \varprojlim D$$

in **Grp**.

Example. We discuss two important examples:

1. Let $(\mathbb{N}, \geq)$ be the poset of all natural numbers with $n \geq m$ iff $m|n$. In categorical language we define $n \to m$ iff $m|n$ (i.e. $n \to m$ iff m is a factor of n). This makes $\mathbb{N}$ a cofiltered poset because any

subset of $\mathbb{N}$ has a maximum element (a cone) in this sense which is just the lcm of all elements of the subset. Now, define the following diagram in $\mathbf{Grp}^{\mathrm{Fin}}$

$$\begin{aligned} D : \mathbb{N} &\longrightarrow \mathbf{Grp}^{\mathrm{Fin}} \\ n &\longmapsto \mathbb{Z}/n\mathbb{Z} \\ n \to m &\longmapsto \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \end{aligned}$$

where the map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ takes $k + n\mathbb{Z}$ to $k + m\mathbb{Z}$ which is obtained by looking at residue by dividing by m. Then the inverse limit $\varprojlim D$ in $\mathbf{Grp}$ is called the **profinite completion** of $\mathbb{Z}$ and is denoted by $\hat{\mathbb{Z}}$.

2. With the same cofiltered poset $(\mathbb{N}, \geq)$ as above, let us consider a prime power q and the following diagram in $\mathbf{Grp}^{\mathrm{Fin}}$

$$\begin{aligned} D : \mathbb{N} &\longrightarrow \mathbf{Grp}^{\mathrm{Fin}} \\ n &\longmapsto \mathbf{Gal}\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right] \\ n \to m &\longmapsto \mathbf{Gal}\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right] \to \mathbf{Gal}\left[\mathbb{F}_{q^m} : \mathbb{F}_q\right] \end{aligned}$$

where the map is defined as

$$\begin{aligned} \mathbf{Gal}\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right] &\to \mathbf{Gal}\left[\mathbb{F}_{q^m} : \mathbb{F}_q\right] \\ \sigma &\mapsto \sigma|_{\mathbb{F}_{q^m}} \end{aligned}$$

which is well defined because $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$ as $m|n$ (Lemma 6.0.5). Finally, the inverse limit $\varprojlim D$ is yet another example of a profinite group.

A possible answer to the of question of why we are putting such a posetal structure on $\mathbb{N}$ above should be indicated by the Lemma 6.0.5, but it will become more clear in the proof of the main theorem below. We now have the following main theorem characterizing the absolute Galois group of a finite field:

Theorem 15. (Characterization of absolute Galois group) Let q be some prime power. Then,

$$\mathbf{Gal}\left[\overline{\mathbb{F}_q} : \mathbb{F}_q\right] \cong \varprojlim_n \mathbf{Gal}\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right].$$

Proof. Consider the natural map

$$\begin{aligned} \theta_n : \mathbf{Gal}\left[\overline{\mathbb{F}_q} : \mathbb{F}_q\right] &\longrightarrow \mathbf{Gal}\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right] \\ \sigma &\longmapsto \sigma|_{\mathbb{F}_{q^n}}. \end{aligned}$$

This is well defined for each n. We will show that the combined map $\theta : \mathbf{Gal}\left[\overline{\mathbb{F}_q} : \mathbb{F}_q\right] \longrightarrow \varprojlim_n \mathbf{Gal}\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right]$ is an isomorphism while implicitly using Proposition 6.1.2. We will also use the explicit description of the projective limit of a cofiltered system as shown in Lemma 3.1.6. First, we show that θ is injective. This is easy, as non-equal $\sigma_1, \sigma_2 \in \mathbf{Gal}\left[\overline{\mathbb{F}_q} : \mathbb{F}_q\right]$ will have non equal restriction in each $\mathbb{F}_{q^n}$. To show surjectivity of θ, take any element $(\sigma_n)_{n\in\mathbb{N}} \in \varprojlim_n \mathbf{Gal}\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right]$. We wish to find an $\mathbb{F}_q$-automorphism of $\overline{\mathbb{F}_q}$ which restricts to each n to σ_n. Consider the following map

$$\begin{aligned} \sigma : \overline{\mathbb{F}_q} &\longrightarrow \overline{\mathbb{F}_q} \\ x &\longrightarrow \sigma_n(x) \text{ if } x \in \mathbb{F}_{q^n}. \end{aligned}$$

We now need to show that this is indeed an automorphism. We first see the main idea of the case when we take two elements in the field which is contained only in the field which contains both their base fields.

The general case has a similar idea. This is indeed an automorphism of $\overline{\mathbb{F}_q}$ in this case because if we take $x \in \mathbb{F}_{q^n}$ and $y \in \mathbb{F}_{q^m}$ then $x + y \in \mathbb{F}_{q^{\text{lcm}(n,m)}}$, which thus means that $\sigma(x + y) = \sigma_{\text{lcm}(n,m)}(x + y)$ and $\sigma_n(x) + \sigma_m(y) \in \mathbb{F}_{q^{\text{lcm}(n,m)}}$, but since there is a map $n \to \text{lcm}\,(n, m)$ and $m \to \text{lcm}\,(n, m)$ in $\mathbb{N}$, hence as in above example, we should have that $\sigma_n|_{\mathbb{F}_{q^{\text{lcm}(n,m)}}} = \sigma_{\text{lcm}(n,m)}$, which finally shows that $\sigma(x + y) = \sigma_{\text{lcm}(n,m)}(x+y) = \sigma_{\text{lcm}(n,m)}(x)+\sigma_{\text{lcm}(n,m)}(y) = \sigma_n(x)+\sigma_m(y)$ which is what we wanted to show. This makes $\sigma \in \textbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$. Similarly one can verify the other axioms of an automorphism. Finally, it's trivial to see that $\theta(\sigma) = (\sigma_n)_{n\in\mathbb{N}}$. This shows θ is surjective and hence makes $\textbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q] \cong \varprojlim_n \textbf{Gal}\,[\mathbb{F}_{q^n} : \mathbb{F}_q]$. ■

It is important to note the map which is establishing this isomorphism; the map θ takes a $(\sigma_n)_{n\in\mathbb{N}} \in \textbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$ to it's restriction on each n. Some easy but interesting corollaries of the above are as below:

Corollary 6.1.4. Let q be some prime power. Then,

$$\textbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q] \cong \hat{\mathbb{Z}}.$$

Proof. Follows easily from Theorem 15, Lemma 6.0.3 and the example above. ■

Corollary 6.1.5. Let q be some prime power. Then,

$$\textbf{Gal}\,[\mathbb{F}_{q^n} : \mathbb{F}_q] = \{\sigma|_{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \mid \sigma \in \textbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]\}.$$

Proof. $\supseteq$ is clear. Take any $\sigma_n \in \textbf{Gal}\,[\mathbb{F}_{q^n} : \mathbb{F}_q]$. By Proposition 1.4.4, since we have an $\mathbb{F}_q$-homomorphism $\sigma_n : \mathbb{F}_{q^n} \to \overline{\mathbb{F}_q}$, we get a $\sigma \in \textbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$ which is an extension of σ_n, whose restriction will trivially be σ_n. ■

There is a distinct member of $\textbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$, which is quite important and will occur very frequently in the generalization of perfect fields to perfect rings (and hence would be important in the study of adic spaces):

Definition 6.1.6. (**Frobenius automorphism of** $[\overline{\mathbb{F}_q} : \mathbb{F}_q]$) Let q be a prime power. For each $n \in \mathbb{N}$, we have a map

$$\begin{aligned} \pi_n : \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_{q^n} \\ x &\longmapsto x^q \end{aligned}$$

which is clearly a member of the $\textbf{Gal}\,[\mathbb{F}_{q^n} : \mathbb{F}_q]$. Hence we have a member $(\pi_n)_{n\in\mathbb{N}} \in \varprojlim_n \textbf{Gal}\,[\mathbb{F}_{q^n} : \mathbb{F}_q] \cong \textbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$. This distinct element $\pi = (\pi_n)_{n\in\mathbb{N}}$ of the absolute Galois group of $\mathbb{F}_q$ is called the Frobenius automorphism of $[\overline{\mathbb{F}_q} : \mathbb{F}_q]$.

Remark 6.1.7. Lemma 6.0.3 tells us that $\pi_n : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $x \mapsto x^q$ is a generator of $\textbf{Gal}\,[\mathbb{F}_{q^n} : \mathbb{F}_q]$.

6.2 Function fields

Let K be a field. A **function field over** K is a field extension of K as in $[F : K]$ which is not algebraic. This is another way of saying that there exists $\alpha \in F$ such that there is no polynomial $f(x) \in K[x]$ whose root is α, or that there is an element in F which is transcendental over K. One also calls the base field K the constant field of function field $[F : K]$. For a function field $[F : K]$, we denote F_{alg} to be the intermediate field extension consisting of all algebraic elements of F over K.

Clearly, a function field cannot be a finite dimensional extension of base field (otherwise it would be algebraic), but it would be quite nice if we could have it as a finite dimensional extension of some other simple object made from the base field. For this purpose, we call a function field $[F : K]$ an **algebraic function field in one variable** if $K = F_{\text{alg}}$ and there exists a transcendental element $\alpha \in F$ such that

F is a finite dimensional (hence algebraic) field extension of the function field of all rational functions[34] $K(\alpha)$ in α. In particular, if the base field K is a finite field, then the algebraic function field in one variable $[F : K]$ is called a **global function field**[35].

We will later see the striking fact that studying algebraic function fields of one variable is equivalent to studying the geometric objects called *non-singular projective curves*. Hence every object developed in this section will have a fairly concrete geometric meaning. This provides us with a good motivation for studying these abstract algebraic objects.

From now on whenever we mention a function field, it is assumed to be and algebraic function field in one variable. Let us now revise what is a discrete valuation on a function field

Definition 6.2.1. (**Valuation on a function field**) Let $[F : K]$ be a function field (in one variable). A valuation on $[F : K]$ is a function

$$v : F \longrightarrow \mathbb{R} \cup \{\infty\}$$

such that

1. $v(z) = \infty$ if and only if $z = 0$,
2. $v(yz) = v(y) + v(z)$ for any $y, z \in F$,
3. $v(y + z) \geq \min\{v(y), v(z)\}$,
4. $v(F^*) \neq \{0\}$, i.e. $\exists y \in F^*$ such that $v(y) \neq 0$,
5. $v(K^*) = \{0\}$, i.e. $\forall y \in K^*$, $v(y) = 0$.

Remark 6.2.2. Some quick axiomatics from the above definition leads to

- v is a group homomorphism as in
$$v : (F^*, \cdot) \longrightarrow (\mathbb{R}, +).$$
- For any $n \in \mathbb{N}$, $v(z^n) = nv(z)$.
- $v(1) = 0$ & $v(-1) = 0$.
- $v(-z) = v(z)$.
- $v(z^{-1}) = -v(z)$.
- If $v(y) \neq v(z)$, then $v(y + z) = \min\{v(y), v(z)\}$. To see this, take any two such $v(y)$ and $v(z)$ and assume WLOG $v(y) < v(z)$. One can then derive $v(y) > v(y)$, a contradiction, by writing $y = (y + z) - z$.

One calls a valuation v of $[F : K]$ **discrete** if the image of non-zero elements $v(F^*)$ is a discrete set in $\mathbb{R}$. One also calls v **normalized** if $v(F^*) = \mathbb{Z}$. Note that any discrete valuation v on $[F : K]$ can be used to construct a normalized valuation by the following construction: we know that $v(F^*)$ is a discrete subset of $\mathbb{R}$, but since $v(F^*)$ is always a subgroup of $(\mathbb{R}, +)$, therefore we can write $v(F^*) = c\mathbb{Z}$ for some $c \in \mathbb{R}$, as is visible by obvious conclusions in Remark 6.2.2 and the fact that there is no non-trivial finite subgroup of $(\mathbb{R}, +)$.

[34] note that it is indeed a function field over K!

[35] It is mentioned in various places in literature that these global function fields have both *geometric* and *arithmetic* flavors. Understanding this sentence is in the making.

6.2.1 Place & it's valuation ring & residue class field

Let $[F : K]$ be a function field. Denote $\mathbf{DV}([F : K])$ to be the set of all discrete valuations on $[F : K]$. For two discrete valuations $v, w \in \mathbf{DV}([F : K])$, the following forms an equivalence relation on $\mathbf{DV}([F : K])$

$$v \sim w \iff \exists c > 0 \text{ s.t. } v(z) = cw(z)\ \forall z \in F^*.$$

We then quotient the set $\mathbf{DV}([F : K])$ by $\sim$ to obtain $\mathbf{Pl}([F : K]) = \mathbf{DV}([F : K]) / \sim$. This set is called the set of **places of function field** $[F : K]$ and an element of $\mathbf{Pl}([F : K])$ is called a **place** of $[F : K]$. The main thing we want to notice is that:

Lemma 6.2.3. Let $[F : K]$ be a function field. Then we have a bijection

$$\mathbf{DV}([F : K])_{\text{norm}} \cong \mathbf{Pl}([F : K]).$$

Proof. As seen earlier, we can convert any discrete valuation to be equivalent (in sense of $\sim$ above) to a normalized valuation. Thus, for each place $P \in \mathbf{Pl}([F : K])$, there is a unique normalized valuation v in P, which thus represents P, and we write v_P to denote this valuation which is a real constant away from all other discrete valuations in P. ■

Out of a function field $[F : K]$, we have constructed collection of objects called places. For each place $P \in \mathbf{Pl}([F : K])$, there is a unique valuation v_P with $v(F^*) = \mathbb{Z}$. Now, the effect of such a v_P is that it gives us a sense of *parity* on the whole field F, as $v(z^{-1}) = -v(z)$, therefore out of z and z^{-1} the valuation v_P has to *choose* which one to assign a positive value and which one to assign a negative value. This motivates the following definition:

Definition 6.2.4. (**Valuation Ring of a Place**) Let $[F : K]$ be a function field and $P \in \mathbf{Pl}([F : K])$ with v_P the corresponding unique normalized valuation. We then define a subring of the field F

$$\mathscr{O}_P := \{z \in F \mid v_P(z) \geq 0\}$$

which is called the valuation ring of the place P.

The above definition selects those elements of the function field which has non-negative value under the discrete valuation v_P. Note that $\mathscr{O}_P$ contains in it the information of the $v_P(z)$ even if $z \notin \mathscr{O}_P$ because by Remark 6.2.2, we know $v_P(z^{-1})$ and $v_P(-z)$, which covers all the non-zero elements of F.

It next turns out that $\mathscr{O}_P$ is a local ring:

Lemma 6.2.5. Let $[F : K]$ be a function field and $P \in \mathbf{Pl}([F : K])$ be a place. The valuation ring $\mathscr{O}_P$ is a local ring with the maximal ideal ideal being

$$\mathfrak{m}_P = \{z \in F \mid v_P(z) \geq 1\}.$$

Proof. $\mathfrak{m}_P$ as above is indeed an ideal by definition of $\mathscr{O}_P$. Take any $z \in F \setminus \mathfrak{m}_P$. We wish to show that z has an inverse in $\mathscr{O}_P$. Clearly $0 \leq v_P(z) < 1$. But since $v_P(F^*) = \mathbb{Z}$ as v_P is normalized, therefore $v_P(z) = 0$. Since $v_P(z^{-1}) = -v_P(z)$, therefore $v_P(z^{-1}) = 0$, and hence $z^{-1} \in F$ is also an element in $F \setminus \mathfrak{m}_P$. Therefore every element outside of $\mathfrak{m}_P$ is invertible. This shows that $\mathscr{O}_P$ is a local ring with maximal ideal $\mathfrak{m}_P$. ■

Another easy result is that $\mathfrak{m}_P$ as above is a principal ideal:

Lemma 6.2.6. Let $[F : K]$ be a function field, $P \in \mathbf{Pl}([F : K])$ be a place and $(\mathscr{O}_P, \mathfrak{m}_P)$ be the valuation local ring. Then

$$\mathfrak{m}_P = \langle z \rangle$$

where $z \in \mathscr{O}_P \subset F$ is such that $v_P(z) = 1$.

Proof. For any $y \in \mathfrak{m}_P$, we have $v_P(y) \geq v_P(z) = 1 \iff v_P(y) - v_P(z) \geq 0 \iff v_P(y) + v_P(z^{-1}) \geq 0 \iff v_P(yz^{-1}) \geq 0$. Therefore $\mathfrak{m}_P \subset \langle z \rangle$. Conversely, for any $yz \in \langle z \rangle$ where $y \in \mathscr{O}_P$, we have that $v_P(yz) = v_P(y) + v_P(z) \geq 1$. ∎

Let us end this section by discussing the residue class field of a place:

Definition 6.2.7. (**Residue Class Field of a Place**) Let $[F : K]$ be a function field. Suppose $P \in \mathbf{Pl}([F : K])$ is some place of this function field. Then, the residue class field of place P is defined to be the residue field of the corresponding local ring:

$$F_P := \mathscr{O}_P/\mathfrak{m}_P.$$

The projection map

$$\begin{aligned} \pi : \mathscr{O}_P &\longrightarrow F_P \\ z &\longmapsto z + \mathfrak{m}_P \end{aligned}$$

is correspondingly called the residue class map of place P.

The main result about this object is that it is a finite extension of constant field K:

Proposition 6.2.8. Let $[F : K]$ be a function field and take any place $Q \in \mathbf{Pl}([F : K])$. The residue class field of Q, F_Q, is a finite extension of K, that is,

$$\dim[F_Q : K] < \infty.$$

Proof. The strategy to prove this is via the usage of the two facts: 1. Every place of $[F : K]$ restricts to a place of $[K(\alpha) : K]$ where α is the transcendental element of F by the definition of a function field, 2. Let P be a place of $[K(\alpha) : K]$, then $\dim[F_P : K] < \infty$. The first of this is trivial, the second is in Section 1.5 of [NX09]. Now, let $Q \in \mathbf{Pl}([F : K])$ and consider it's restriction to $[K(\alpha) : K]$. We first observe that there is an isomorphic copy of $\mathscr{O}_P/\mathfrak{m}_P$ inside $\mathscr{O}_Q/\mathfrak{m}_Q$ because of the following field morphism (remember $\mathfrak{m}_P \subseteq \mathfrak{m}_Q$ by Lemma 6.2.5):

$$\begin{aligned} \mathscr{O}_P/\mathfrak{m}_P &\longrightarrow \mathscr{O}_Q/\mathfrak{m}_Q \\ z + \mathfrak{m}_P &\longmapsto z + \mathfrak{m}_Q. \end{aligned}$$

We want to use the fact that $\dim[F : K(\alpha)] < \infty$ in a useful manner. For this, first note that $\dim[F_Q : K] = \dim[F_Q : F_P] \times \dim[F_P : K]$ by basic vector space arguments. We already know by above that $\dim[F_P : K] < \infty$, so we reduce to the task of showing that $\dim[F_Q : F_P] < \infty$. For this, we just observed that an isomorphic copy of F_P is inside F_Q. So we reduce to showing that an F_P-linearly independent collection $\{z_i + \mathfrak{m}_Q\}$ of $[F_Q : F_P]$ gives a $K(\alpha)$-linearly independent collection $\{z_i\}$ of $[F : K(\alpha)]$. Suppose conversely that $\{z_i + \mathfrak{m}_Q\}$ is a linearly independent collection in $[F_Q : F_P]$ but $\{z_i\}$ is al linearly dependent collection in $[F : K(\alpha)]$. Then, suppose $\sum c_i z_i = 0$ in F where $c_i \in K(\alpha)$. Upto rearrangement, we can assume c_1 is such that $v_P(c_1) = \min_{1 \leq i \leq n} v_P(c_i)$. Now, since c_i are in field $K(\alpha)$, then one can always write,

$$z_1 + \sum (c_1^{-1} c_i) z_i = 0$$

where, since $c_i c_1^{-1} \in K(\alpha)$ is such that $v_P(c_i c_1^{-1}) = v_P(c_i) - v_P(c_1) \geq 0$, we get that $v_P(b_i b_1^{-1}) \geq 0$ and thus $b_i b_1^{-1} \in \mathscr{O}_P$ (note that $v_P(x) \geq 0 \forall x \in K(\alpha)$ because of the way $K(\alpha)$ is constructed from K and $v_P(K) = \{0\}$ by definition), we thus get by quotienting out by $\mathfrak{m}_Q$ that $\{z_i + \mathfrak{m}_Q\}$ is a linearly dependent set, which is a contradiction. ∎

One thus defines the degree of a place as follows:

Definition 6.2.9. (**Degree of a Place**) Let $[F : K]$ be a function field and let $P \in \mathbf{Pl}([F : K])$ be a place. The degree of the place P is defined to be:

$$\deg P := \dim [\mathscr{O}_P/\mathfrak{m}_P : K]$$

which is finite by Proposition 6.2.8. A place P of $[F : K]$ is called to be rational if $\deg P = 1$.

We will later see that the degree of a place of the function field of a non-singular projective curve over $\mathbb{F}_q$ is equal to the degree of the corresponding $\mathbb{F}_q$-closed point of the curve.

6.2.2 The $v_{p(x)}$ & v_∞ over rational functions

Let $[F : K]$ be a function field and let $\alpha \in F$ be the element which makes F a finite extension of $K(\alpha)$. The field of rational functions $K(\alpha)$ is itself a function field over K as it contains the transcendental element $\alpha \in F$ and, in-fact, $K(\alpha)_{\text{alg}} = K$ as any other rational fraction formed by α cannot possibly be algebraic. So we have an important function field (algebraic, one-variable) $[K(\alpha) : K]$ obtained by another function field (algebraic, one-variable) $[F : K]$.

Our goal in this section is to characterize each place of $[K(\alpha) : K]$. We now define two important normalized valuations on this function field $[K(\alpha) : K]$ derived from the function field $[F : K]$, which will help us in this characterization:

Definition 6.2.10. (**Valuation** $v_{p(x)}$) Let $[F : K]$ be a function field with the transcendental element for F being $\alpha \in F$. Let $p(x)$ be a monic irreducible polynomial in $K[x]$. The following is a recursive definition of a well-defined normalized valuation on the function field $K(\alpha)$

$$\begin{aligned} v_{p(x)} : K(\alpha) &\longrightarrow \mathbb{R} \cup \{\infty\} \\ \frac{f(\alpha)}{g(\alpha)} &\longmapsto \begin{cases} m & \text{if } g(x) = 1 \ \&\ m \in \mathbb{N} \cup \{0\} \text{ is largest s.t. } p^m(x) | f(x), \\ v_{p(x)}(f(x)) - v_{p(x)}(g(x)) & \text{if } g(x) \neq c \text{ (constant in } K), \\ \infty & \text{if } f(x) = 0. \end{cases} \end{aligned}$$

Remark 6.2.11. We don't distinguish between $K(\alpha)$ and $K(x)$ above. This is because $K(\alpha)$, as mentioned earlier, is a function field over K, hence $K(\alpha)_{\text{alg}} = K$. Hence $K(\alpha)$ becomes isomorphic to $K(x)$, the field of fractions of the polynomial domain $K[x]$. We will implicitly do calculations without regard to this *syntactic* distinction.

The fact that this is a valuation follows easily from Definition 6.2.1, in particular, if you multiply two polynomials each of which has some power of $p(x)$ as a factor, then so does the product with the power on $p(x)$ being both their sum. Similarly, one can see the corresponding about sum of two such polynomials. $v_{p(x)}$ is normalized because it takes values only in $\mathbb{Z}$.

Moving on, we have another valuation on $K(\alpha)$, the v_∞:

Definition 6.2.12. (**Valuation** v_∞) Let $[F : K]$ be a function field with the transcendental element for F being $\alpha \in F$. The following is a well-defined normalized valuation on the function field $K(\alpha)$

$$\begin{aligned} v_\infty : K(\alpha) &\longrightarrow \mathbb{R} \cup \{\infty\} \\ \frac{f(\alpha)}{g(\alpha)} &\longmapsto \deg g(x) - \deg f(x). \end{aligned}$$

The corresponding DVR $\mathscr{O}_\infty \subset K(\alpha)$ consists of all rational functions of the form

$$\mathscr{O}_\infty = \left\{ \frac{f(x)}{g(x)} \in K(\alpha) \mid \deg g(x) \geq \deg f(x) \right\}$$

and the maximal ideal $\mathfrak{m}_\infty$ will be those fractions with degree of denominator being strictly greater than that of numerator. The local parameter of this DVR is any fraction $1/f(x)$ where $f(x)$ is of degree 1. Also note that $\mathscr{O}_\infty/\mathfrak{m}_\infty \cong k$ via the mapping $\mathscr{O}_\infty \longrightarrow k$ such that $\frac{c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0}{x^d + b_{d-1}x^{d-1} + \cdots + b_0} \mapsto c_d$ where c_i are allowed to be zero.

Again, this indeed is a normalized valuation on $K(\alpha)$ because of similar reasons which makes $v_{p(x)}$ such. It turns out that these are exactly all the places of rational function field $[K(\alpha) : K]$. Let us state this theorem now:

Theorem 16. Let $[K(\alpha) : K]$ be a rational function field. Then, each place of $[K(\alpha) : K]$ is either of the form $v_{p(x)}$ for $p(x) \in K[x]$ being a monic irreducible polynomial, or v_∞.

Proof. Let us work out how the characterization of $v_{p(x)}$ arises and we will leave out the proof of v_∞ to be referred from the proof of Theorem 1.5.8 of [NX09]. Given is the rational function field $[K(\alpha) : K]$. The classification begins by taking any discrete valuation $v \in \mathbf{DV}([K(\alpha) : K])$. In order to show that it is equivalent to $v_{p(x)}$, we have to show that $\exists c \in \mathbb{R},\ v(r(x)) = cv_{p(x)}(r(x))$ for all $r(x) \in K(\alpha)$. We now divide into two cases, when $v(\alpha) \geq 0$ and when $v(\alpha) < 0$. We focus on the former. Denote the corresponding place of v to be $P \in \mathbf{Pl}([K(\alpha) : K])$. To show that P contains a $v_{p(x)}$. Suppose $v(\alpha) \geq 0$, therefore $\alpha \in \mathscr{O}_P \subseteq K(\alpha)$. In particular, for any $f(x) \in K[x]$, $v(f(x)) \geq 0$ by axioms of valuation. Therefore, the entire $K[x]$ is embedded in $\mathscr{O}_P$, that is $K[x] \subseteq \mathscr{O}_P$. Now, we know that $\mathscr{O}_P$ is a local ring, so it's maximal ideal, $\mathfrak{m}_P$, gives the following maximal ideal of $K[x]$, $K[x] \cap \mathfrak{m}_P$. Call this maximal ideal $I \subseteq K[x]$. Since $K[x]$ is principal so $\exists p(x) \in K[x]$ which is monic irreducible so that $\langle p(x) \rangle = I$. We now claim that $v_{p(x)}$ is equivalent to v. For this, take any $r(x) \in K(\alpha)$. Suppose $r(x) = p(x)^m \frac{f(x)}{g(x)}$ where $f(x)$ and $g(x)$ doesn't have $p(x)$ as a factor. Then

$$v\left(p(x)^m \frac{f(x)}{g(x)}\right) = v(p(x)^m) + v\left(\frac{f(x)}{g(x)}\right) = mv(p(x))$$

where $v\left(\frac{f(x)}{g(x)}\right) = v(f(x)) - v(g(x))$, but since $f(x), g(x) \notin \mathfrak{m}_P$ because $f(x), g(x) \notin \langle p(x) \rangle = I = K[x] \cap \mathfrak{m}_P$, therefore $v(f(x)) = v(g(x)) = 0$ by definition of the maximal ideal of the valuation ring of a place. Thus, we get

$$v\left(p(x)^m \frac{f(x)}{g(x)}\right) = mv(p(x)) = v_{p(x)}(r(x)) \cdot v(p(x)) = cv_{p(x)}(r(x))$$

where $c := v(p(x))$ is a strictly positive constant; it cannot be zero because $p(x) \in K[x] \cap \mathfrak{m}_P \subset \mathfrak{m}_P$. Thus, $v_{p(x)}$ is in place P of v. ∎

6.2.3 Discrete valuation rings

Let us end this section by another important object that will pop up again in the discussion of curves, but has a subtle connection with valuation rings; valuations arise naturally from such rings. One may call that DVRs are generalization of the phenomenon of valuation ring of a place (Definition 6.2.4).

Definition 6.2.13. (**Discrete Valuation Ring**) Let R be an integral domain. If there exists an irreducible element $t \in R$ such that for each element $z \in R$, there exists an unit element $u \in R$ and $n \in \mathbb{N}$ such that $z = ut^n$, then R is called a discrete valuation ring (DVR). The distinguished element $t \in R$ is then called the local parameter of the DVR R.

The following result is a basic consequence of the definition:

Lemma 6.2.14. Every DVR R with the local parameter t is a local ring with the unique maximal ideal being $\{ut^n \mid u \in R \text{ is unit } \& \ n \geq 1\} \cup \{0\}$, i.e. $\mathfrak{m}$ is the ideal of all non-units of R. In-fact, this maximal ideal is the only proper prime ideal of R, which means that $\dim R = 1$. ■

Another important result about DVRs is that there is no DVR between one DVR and it's field of fractions:

Lemma 6.2.15. Let R and S be DVRs such that $R \subseteq S \subseteq R_{\langle 0 \rangle}$. Then, $R = S$.

Proof. We just have to show that $S \subseteq R$. For this, first let $k \in S$ and $t \in R$ be the local parameters of the rings respectively. Suppose that $R \subset S$ and thus $x \in S \setminus R$. We can write x as an element of S and also as an element of $R_{\langle 0 \rangle}$. One can also write $t \in R$ in the form of $k \in S$. Reconciling these three forms of x leads to a contradiction. ■

Now, for a local ring $(R, \mathfrak{m})$, one can understand the ring $\mathfrak{m}/\mathfrak{m}^2$ as an $R/\mathfrak{m}$-vector space by the following well-defined action:

$$\begin{aligned} R/\mathfrak{m} \times \mathfrak{m}/\mathfrak{m}^2 &\longrightarrow \mathfrak{m}/\mathfrak{m}^2 \\ \big(r + \mathfrak{m}, m + \mathfrak{m}^2\big) &\longmapsto (rm + \mathfrak{m}^2). \end{aligned}$$

Usually one denotes the residue field $R/\mathfrak{m}$ of local ring by κ. So $\mathfrak{m}/\mathfrak{m}^2$ is a κ-vector space.

We have another important characterization of DVRs which tells us when a local Noetherian ring of dimension 1 is a DVR:

Lemma 6.2.16. Let $(R, \mathfrak{m})$ be a local Noetherian ring of Krull dimension 1 with residue field κ. Then, $(R, \mathfrak{m})$ is a DVR if and only if the dimension of the κ-vector space $\mathfrak{m}/\mathfrak{m}^2$ is 1.

Proof. (L $\implies$ R) Let $(R, \mathfrak{m})$ be a DVR. Since $\mathfrak{m} = tR$, therefore $\mathfrak{m}^2 = t^2R$. Thus,

$$\mathfrak{m}/\mathfrak{m}^2 = tR/t^2R \cong R/tR = \kappa.$$

(R $\implies$ L) Take the basis element $t + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$. In particular this implies that $t \in \mathfrak{m}$ but $t \notin \mathfrak{m}^2$. Remember $(R, \mathfrak{m})$ is a local Noetherian ring of dimension 1. Therefore $\mathfrak{m}$ is the only proper prime ideal of R. By Lemma 6.2.14, we see that $\mathfrak{m}$ consists of non-units of R and this forms a prime ideal. This means each element of $\mathfrak{m}$ is irreducible because for any factorization $t = fg$, either $f \in \mathfrak{m}$ or $g \in \mathfrak{m}$, which translates to either f is a non-unit or g is a non-unit, but if both becomes non-unit then $t \in \mathfrak{m}^2$, which cannot happen. It is a result that we can now safely say that $\mathfrak{m}$ is principal[36]. Thus it has to be the case that $\mathfrak{m} = tR$ as t is irreducible and $\mathfrak{m}$ contains all non-units and t generates that ideal. If from here we can show that R has unique factorization, then we will be done. It turns out by commutative algebra that R of dimension 1 with only one prime ideal which is maximal is a UFD. This completes the proof. ■

The interesting thing about DVRs is that they come equipped with a **natural valuation** on them. In particular, let R be a DVR and consider the following map from the fraction field of R:

$$\begin{aligned} \operatorname{ord}(-) : R^*_{\langle 0 \rangle} &\longrightarrow \mathbb{Z} \\ ut^m &\longmapsto m. \end{aligned}$$

Also, consider $\operatorname{ord}(0) = \infty$. Now compare this with the axioms in Definition 6.2.1. We see that $\operatorname{ord}(yz) = \operatorname{ord}(y) + \operatorname{ord}(z)$, $\operatorname{ord}(y+z) \geq \min\{\operatorname{ord}(y), \operatorname{ord}(z)\}$ and of-course, the image of $\operatorname{ord}(-)$ is non-zero. This means that $\operatorname{ord}(-)$ is a discrete valuation on the fraction field of the DVR R, $R_{\langle 0 \rangle}$.

Let us further make the following observation:

[36] This is akin to Lemma 6.2.6.

Lemma 6.2.17. Let $[F : K]$ be a function field (algebraic, one-variable) and let $P \in \mathbf{Pl}([F : K])$ be a place. The valuation ring of P, $\mathscr{O}_P$, is a DVR.

Proof. By Lemmas 6.2.5 and 6.2.6 , we know that $(\mathscr{O}_P, \mathfrak{m})$ is a local ring where $\mathfrak{m} = \{z \in F^* \mid v_P(z) \geq 1\}$ and moreover, that $\mathfrak{m}$ is principal, where $\mathfrak{m} = \langle t \rangle$ where $v_P(t) = 1$. Now, we know that this $t \in F^*$ is irreducible because if it is not, then it will not be able to generate the maximal ideal $\mathfrak{m}$. We thus reduce to showing that every element of $\mathscr{O}_P$ is of form ut^m for some unit $u \in \mathscr{O}_P$ and $m \in \mathbb{N}$. Take any $z \in \mathscr{O}_P$. If $z \notin \mathfrak{m}$, then it is necessarily a unit. Thus we reduce to the case when $z \in \mathfrak{m}$. We know that $v_P(z) \geq 1$, say $v_P(z) = m \geq 1$, in this case. But, since every such z is necessarily in $\mathfrak{m}$, thus $z = ut^m$ for some $u \notin \mathfrak{m} = \langle t \rangle$ which are also necessarily invertible as $(\mathscr{O}_P, \mathfrak{m})$ is a local ring. ■

It is in the sense of above lemma do we say that DVRs generalize the notion of valuation rings of a place because these later objects are particular instances of DVRs, as developed in this section.

7 Review of algebraic geometry

We finally come to the interesting part of the theory of finite fields, that of it's geometry. Doing geometry over finite fields is a bit different than usual, in particular, the absolute Galois group of the finite field plays a central role in the dynamics of various objects defined over them. Hence, we will develop it while having this Galois group in mind, but not limited by it.

First, some trivial things. Let k be a perfect field. In-fact we will always denote k to be a perfect field. Denote $\mathbb{A}^n := \mathbb{A}^n(\overline{k})$ to be the collection of all n-tuples of closure of field k. This is the affine n-space over k. If $[K : k]$ is a finite extension, then a point of the space $\mathbb{A}^n(K)$ is called **K-rational**. If a point $P \in \mathbb{A}^n(K)$ is such that each of it's component is in k, then P is also said to be k-rational or just a **rational point of** $\mathbb{A}^n(K)$.

Let us now draw Galois group into the picture:

Lemma 7.0.1. Let $\mathbf{Gal}\,[\overline{k} : k]$ be the absolute Galois group of k. The affine n-space $\mathbb{A}^n$ is a $\mathbf{Gal}\,[\overline{k} : k]$-set by the map

$$\begin{aligned}\mathbf{Gal}\,[\overline{k} : k] \times \mathbb{A}^n &\longrightarrow \mathbb{A}^n \\ (\sigma, (a_1, \ldots, a_n)) &\longmapsto (\sigma(a_1), \ldots, \sigma(a_n)).\end{aligned}$$

Proof. Trivially follows unitality and associativity. ■

Since the Frobenius $\pi \in \mathbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$ is the generator (Remark 6.1.7), so it's fixed field by fundamental theorem has to be $\mathbb{F}_q$. So if $k = \mathbb{F}_q$ for some prime power q, then we can characterize the rational points of $\mathbb{A}^n$ by just finding all those points $P \in \mathbb{A}^n$ which are fixed by π. In more formal words, we have proved

Lemma 7.0.2. Let $k = \mathbb{F}_q$ be a finite field and $\pi \in \mathbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$ be the Frobenius. Then, we have the trivial bijection

$$\{P \in \mathbb{A}^n \mid P \text{ is rational}\} \cong \{P \in \mathbb{A}^n \mid \pi(P) = P\}.$$

Proof. Proved above/trivial. ■

Now let k again be any field. We can define for each point $P \in \mathbb{A}^n$ the orbit of P by the Galois action of $[\overline{k} : k]$ as in Lemma 7.0.1

$$\mathrm{Cl}\,(P) := O_P = \{\sigma(P) \in \mathbb{A}^n \mid \sigma \in \mathbf{Gal}\,[\overline{k} : k]\}.$$

One calls this orbit $\mathrm{Cl}\,(P)$ the **closed point of P over k** or a k-closed point of $\mathbb{A}^n$. As usual, two members of the orbit $\mathrm{Cl}\,(P)$ are called **conjugate**.

The Galois action of $[\overline{\mathbb{F}_q} : \mathbb{F}_q]$ on $\mathbb{A}^n$ will play a critical role for us. First, for a finite fields $\mathbb{F}_q$, any $\mathbb{F}_q$-closed point is finite

Lemma 7.0.3. Let $\mathbb{F}_q$ be a finite field and $\mathrm{Cl}\,(P)$ be some $\mathbb{F}_q$-closed point. Then $\mathrm{Cl}\,(P)$ is finite.

Proof. Let $P = (a_1, \ldots, a_n) \in \mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{F}_q})$ be a point. Take $\sigma = (\sigma_k)_{k\in\mathbb{N}} \in \mathbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$. Suppose $a_i \in \mathbb{F}_{q^{m_i}}$ for each $i = 1, \ldots, n$. This means that $\sigma(P) = (\sigma_{m_1}(a_1), \sigma_{m_2}(a_2), \ldots, \sigma_{m_n}(a_n))$. Now, each of a_i is contained in $\mathbb{F}_{q^h}$, $h = \mathrm{lcm}\,(m_1, \ldots, m_n)$, so all such elements of $\mathbb{A}^n$ conjugate to P are in $\mathbb{F}_{q^h}$. But this means we are just asking the cardinality of $\{\sigma(P) \in \mathbb{A}^n \mid \sigma \in \mathbf{Gal}\,[\mathbb{F}_{q^h} : \mathbb{F}_q]\}$, i.e. the orbit of P via action of $\mathbf{Gal}\,[\mathbb{F}_{q^h} : \mathbb{F}_q]$, which is finite as this Galois group is finite. ■

Remark 7.0.4. The Lemma 7.0.3 tells us that for a finite field, the number of conjugates of any point is finite in amount. We call the number of conjugates, i.e. $|\mathrm{Cl}\,(P)|$, the **degree of the k-closed point** $\mathrm{Cl}\,(P)$, usually denoted as $\deg \mathrm{Cl}\,(P)$.

Remark 7.0.5. The degree of a closed point $\mathrm{Cl}\,(P)$ for $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(\overline{\mathbb{F}_q})$ can be given in two ways: let $\pi \in \mathbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$ be the Frobenius, then

$$\begin{aligned}\deg \mathrm{Cl}\,(P) &= \text{the smallest integer } m \text{ s.t. } \pi^m(P) = P \\ &= \text{the smallest integer } m \text{ s.t. } a_i \in \mathbb{F}_{q^m} \forall i = 1, \ldots, n.\end{aligned}$$

The proof of this follows a general method which is usually employed to prove that for $a \in \overline{\mathbb{F}_q}$, the conjugates of a are exactly $\pi(a), \pi^2(a), \ldots, \pi^{m-1}(a)$ where $a \in \mathbb{F}_{q^m}$ and m is least such. The proof critically relies on seeing the such $\mathbb{F}_{q^m}$ is necessarily $\mathbb{F}_q(a)$.

Remark 7.0.6. (**Definition field of a point/closed point**) Let k be a (perfect) field and consider the Galois group $\mathbf{Gal}\,[\overline{k} : k]$. Let $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(\overline{k})$. The field of fractions at P, $k(a_1, \ldots, a_n)$, is defined to be the definition field of point P.
In the case when $k = \mathbb{F}_q$, any point $P = (a_1, \ldots, a_n)$ in the affine n-space $\mathbb{A}^n(\overline{\mathbb{F}_q})$ carries also a closed point over it, $\mathrm{Cl}\,(P)$, which is the orbit of action of $\mathbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$ at P. It follows by elementary observations that $\mathbb{F}_q(Q) = \mathbb{F}_q(Q')$ for any $Q, Q' \in \mathrm{Cl}\,(P)$. Hence, instead of asking about the definition field of a given point, one can equivalently ask about the definition field of the closed point over that point.

Our main background space is $\mathbb{A}^n(\overline{\mathbb{F}_q})$. This does not have finitely many points. Keep in mind that this is a $\mathbf{Gal}\,[\overline{\mathbb{F}_q} : \mathbb{F}_q]$-set. What we are pointing at is an apparent build up to an application of Grothendieck's Galois theory. The seed is sown very deep, so it will take time for a plant to grow out of it. In the meantime, we will continue to learn the algebraic geometry over arbitrary fields, and what does algebraic curves over it look like, and then specialize to the case of finite fields.

Let us now discuss projective n-spaces. These are formed by identifying *straight lines* from the affine $n+1$-space. More formally:

Definition 7.0.7. (**Projective n-space**) Let k be a field. The projective n-space $\mathbb{P}^n := \mathbb{P}^n(\overline{k})$ over k is constructed from $\mathbb{A}^{n+1}(\overline{k})$ by quotienting it with the following equivalence relation

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \iff \exists \lambda \neq 0 \in \overline{k} \text{ s.t. } a_i = \lambda b_i \ \forall i = 0, \ldots, n.$$

For a point $P = [a_i]_{i=0}^n$ in $\mathbb{P}^n$, we call a_i the homogeneous coordinates of P. Generalizing from the affine case, for a finite extension $[K : k]$, a point $[a_i] \in \mathbb{P}^n$ is called **K-rational** if there exists $\lambda \in \overline{k}$ such that $[\lambda a_i]$ is point whose each homogeneous coordinate λa_i lies in K. A k-rational point $P = [a_i]$ is said to be simply **rational**.

As usual, we are interested in finite fields, hence in $\mathbb{P}^n(\overline{\mathbb{F}_q})$. Since $\mathbb{A}^{n+1}(\overline{\mathbb{F}_q})$ has finitely many rational points (q^{n+1} to be exact), therefore the quotient $\mathbb{P}^n(\overline{\mathbb{F}_q})$ will also have finitely many rational points. How many exactly is answered by the following simple lemma:

Lemma 7.0.8. Let $\mathbb{F}_q$ be a finite field and consider the projective n-space $\mathbb{P}^n(\overline{\mathbb{F}_q})$ over $\mathbb{F}_q$. There are $\frac{q^{n+1}-1}{q-1}$ non-zero rational points in $\mathbb{P}^n(\overline{\mathbb{F}_q})$.

Proof. It follows that we can reduce to the question of finding the number of equivalence classes in $\mathbb{A}^{n+1}(\mathbb{F}_q)$ under the equivalence relation

$$(a_i)_{i=0}^n \sim (b_i)_{i=0}^n \iff \exists \lambda \neq 0 \in \mathbb{F}_q \text{ s.t. } \lambda a_i = b_i \forall i = 0, \ldots, n.$$

Take any non-zero $(a_i)_{i=0}^n \in \mathbb{A}^{n+1}(\mathbb{F}_q)$. Then for each non-zero $\lambda \in \mathbb{F}_q$, we have a distinct $(\lambda a_i) \in \mathbb{A}^{n+1}(\mathbb{F}_q)$. Hence size of each equivalence class is $q-1$. Denote k to be the number of all classes. Since there are q^{n+1} points in $\mathbb{A}^{n+1}(\mathbb{F}_q)$, we therefore have $q^{n+1} = 1 + k(q-1)$ where 1 corresponds to the size of class of all-zero point. We hence get k as required. ∎

As before, we see that the projective n-space over a field k is a $\mathbf{Gal}\ [\overline{k} : k]$-set:

Lemma 7.0.9. Let k be a (perfect) field and $\mathbf{Gal}\ [\overline{k} : k]$ it's absolute Galois group. The projective n-space $\mathbb{P}^n(\overline{k})$ is a $\mathbf{Gal}\ [\overline{k} : k]$-set.

Proof. Define the action as

$$\begin{aligned} \mathbf{Gal}\ [\overline{k} : k] \times \mathbb{P}^n(\overline{k}) &\longrightarrow \mathbb{P}^n(\overline{k}) \\ (\sigma, [a_i]_{i=0}^n) &\longmapsto [\sigma(a_i)]_{i=0}^n \end{aligned}$$

and observe that this is well-defined for each class and is unital and associative. ■

Remark 7.0.10. (**The Frobenius action on $\mathbb{P}^n(\overline{\mathbb{F}_q})$**) Let $\mathbb{F}_q$ be a finite field and consider the projective n-space $\mathbb{P}^n(\overline{\mathbb{F}_q})$ over it. The Frobenius action on $\mathbb{P}^n(\overline{\mathbb{F}_q})$ is an important action given by

$$\begin{aligned} \pi([a_i]_{i=0}^n) &= [\pi(a_i)]_{i=0}^n \\ &= [a_i^q]_{i=0}^n. \end{aligned}$$

As usual, this is well defined for any point $[a_i] \in \mathbb{P}^n(\overline{\mathbb{F}_q})$.

As usual, for a field k and $\mathbb{P}^n(\overline{k})$, the rational points of $\mathbb{P}^n(k)$ are in bijection with the points fixed by each member of $\mathbf{Gal}\ [\overline{k} : k]$. This follows from fundamental theorem.

Remark 7.0.11. (**Closed point over a point**) Let $P = [a_i] \in \mathbb{P}^n(\overline{k})$ be a point of the projective n-space. We can extend the notion of the closed point from affine to projective case, using the same definition; the orbit of $\mathbf{Gal}\ [\overline{k} : k]$ at P is defined to be the closed point over P. That is,

$$\mathrm{Cl}\,(P) := \{\sigma(P) \in \mathbb{P}^n(\overline{k}) \mid \sigma \in \mathbf{Gal}\ [\overline{k} : k]\}.$$

As usual, $Q, Q' \in \mathrm{Cl}\,(P)$ are called **conjugate**. We also call the cardinality $|\mathrm{Cl}\,(P)|$ as the **degree of the closed point** $\mathrm{Cl}\,(P)$

We have that closed points in $\mathbb{P}^n(\overline{\mathbb{F}_q})$ are also finite:

Lemma 7.0.12. Let $\mathbb{F}_q$ be a finite field and $\mathrm{Cl}\,(P)$ be some closed point in $\mathbb{P}^n(\overline{\mathbb{F}_q})$. Then $\mathrm{Cl}\,(P)$ is finite; $\deg \mathrm{Cl}\,(P) < \infty$.

Proof. As in Lemma 7.0.3. ■

Remark 7.0.13. (Definition field of a point/closed point in $\mathbb{P}^n(\overline{k})$) Let $P = [a_i]$ be a point of $\mathbb{P}^n(\overline{k})$ where for some $0 \leq k \leq n$, $a_k \neq 0$. The definition field of P is defined to be the field of fractions $k(a_0/a_k, \ldots, a_n/a_k)$. It follows that definition field of two conjugate elements is same when $k = \mathbb{F}_q$. Hence we can alternatively talk about definition field of a closed point in $\mathbb{P}^n(\overline{\mathbb{F}_q})$.

There are few main objects which we have defined here on $\mathbb{A}^n(\overline{k})$ and $\mathbb{P}^n(\overline{k})$. Namely, (let $[K : k]$ be an extension)

- k-rational points.
- K-rational points.
- k-closed points over a point and it's degree.
- Definition field of a point.

The applications of algebraic geometry in cryptosystems uses critically the various methods to find $\mathbb{F}_q$-rational points of algebraic curves (we will study them soon). So this is the reason why we are emphasizing on K-rational points on various objects drawn on affine/projective n-space. We will keep these in mind from now on while developing geometry over finite fields.

7.1 Algebraic varieties

We assume that the reader is aware of usual definitions that are encountered in the study of algebraic sets, like the ideals they generate, Hilbert's basis theorem & Nullstellensatz. In any case, here's a quick introduction.

Let k be a (perfect) field. Take any subset $S \subset \overline{k}[x_1, \ldots, x_n]$. The set

$$Z(S) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n(\overline{k}) \mid f(a_1, \ldots, a_n) = 0 \forall f \in S\}$$

defines a subset of the affine n-space $\mathbb{A}^n(\overline{k})$. This is called an **affine algebraic set**. It is usually denoted by V/k and read as "algebraic set V over k". Note that

$$Z(S) = Z(\langle S \rangle)$$

where $\langle S \rangle \subseteq k[x_1, \ldots, x_n]$ is the ideal generated by S. **Hilbert's basis theorem** says that any algebraic set $V \subseteq \mathbb{A}^n(\overline{k})$ is the zero set of finitely many polynomials (equivalently, of a finitely generated ideal of $k[x_1, \ldots, x_n]$).

Let $V \subseteq \mathbb{A}^n(\overline{k})$ be an algebraic set. We define

$$I(V) := \{f \in \overline{k}[x_1, \ldots, x_n] \mid f(P) = 0 \; \forall P \in V\}$$
$$I(V/k) := \{f \in k[x_1, \ldots, x_n] \mid f(P) = 0 \; \forall P \in V\}$$

This gives a subset of $k[x_1, \ldots, x_n]$ which can easily be seen to form an ideal. Let $\mathfrak{a} \subset \overline{k}[x_1, \ldots, x_n]$ be an ideal. **Hilbert's Nullstellensatz** says that

$$I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

We also have the following trivial relations:

Lemma 7.1.1. Suppose $\mathbb{A}^n(\overline{k})$ is the affine n-space over field k and A, B are two algebraic sets and $\{C_i\}_{i \in I}$ is a family of algebraic sets in $\mathbb{A}^n(\overline{k})$. We then have the following:

1. ϕ and $\mathbb{A}^n(\overline{k})$ is algebraic.
2. $A \cup B$ is algebraic.
3. $\cap_{i \in I} C_i$ is algebraic.

Proof. $\phi = Z(1)$ and $\mathbb{A}^n(\overline{k}) = Z(0)$. If $Z(Y_A) = A$ and $Z(Y_B) = B$, then $Z(Y_A \cdot Y_B) = A \cup B$ where $Y_A \cdot Y_B = \{f \cdot g \mid f \in Y_A \;\&\; g \in Y_B\}$. Take any $P \in Z(Y_A \cdot Y_B)$, then $h(P) = 0 \; \forall \; h \in Y_A \cdot Y_B$. But $h \in Y_A \cdot Y_B$ implies $h = f \cdot g$ for some $f \in Y_A$ and $g \in Y_B$. Therefore $h(P) = f(P) \cdot g(P) = 0$ implies $f(P) = g(P) = 0$ as $f(P)$ and $g(P)$ are elements of the field k. Since h iterates over all elements of $Y_A \cdot Y_B$, which in-turn implies all $f \in Y_A$ and all $g \in Y_B$ are such that $f(P) = g(P) = 0$, therefore $P \in A \cup B$.
Conversely, let $P \in A \cup B$. Then $\forall \; f \in Y_A$ and $\forall \; g \in Y_B$, $f(P) = g(P) = 0$. But this implies that $f(P) \cdot g(P) = 0 \forall \; f \in Y_A \; , \;\; g \in Y_B$, that is $P \in Z(Y_A \cdot Y_B)$.
Finally, $\cap_{i \in I} C_i = Z\left(\bigcup_{i \in I} Y_{C_i}\right)$. ∎

Remark 7.1.2. The topology on $\mathbb{A}^n(\overline{k})$ where closed sets are algebraic sets is usually called the Zariski topology on $\mathbb{A}^n(\overline{k})$. Note that open sets in this space, on an intuitive level, are *too big*.

This was some basic algebraic geometry. We however are interested in the finite field case, i.e. when $k = \mathbb{F}_q$. For this, we first study the action of Galois group $\mathbf{Gal}\,[\overline{k} : k]$ on $k[x_1, \ldots, x_n]$ and how it relates to trivial action on $\mathbb{A}^n(\overline{k})$.

Remark 7.1.3. Note that the map

$$\begin{aligned}\textbf{Gal}\,[\overline{k}:k]\times\overline{k}[x_1,\ldots,x_n] &\longrightarrow \overline{k}[x_1,\ldots,x_n]\\ \left(\sigma,\sum a_i x_1^{i_1}\ldots x_n^{i_n}\right) &\longmapsto \sum\sigma(a_i)x_1^{i_1}\ldots x_n^{i_n}\end{aligned}$$

makes $\overline{k}[x_1,\ldots,x_n]$ a $\textbf{Gal}\,[\overline{k}:k]$-set. Moreover, for any $\sigma\in\textbf{Gal}\,[\overline{k}:k]$, $P\in\mathbb{A}^n(\overline{k})$ and $f(x)\in\overline{k}[x_1,\ldots,x_n]$, we have the following easy formula:

$$\sigma(f(P))=\sigma(f)(\sigma(P))$$

where $\sigma(f)$ is defined as above.

The following is an easy, but an eye-raising result, in particular, it shows the importance of the definitions introduced in the previous section.

Lemma 7.1.4. Let k be a (perfect) field and consider an affine algebraic set $V\subseteq\mathbb{A}^n(\overline{k})$. If $P\in V$ is a point in V, then every $Q\in\mathrm{Cl}\,(P)$ is also in V.

Proof. Write $V=Z(\mathfrak{a})$ for some $\mathfrak{a}\subseteq k[x_1,\ldots,x_n]$. If $P\in V$ then $f(P)=0\ \forall f\in\mathfrak{a}$. Take $Q\in\mathrm{Cl}\,(P)$, so for some $\sigma\in\textbf{Gal}\,[\overline{k}:k]$, we write $\sigma(Q)=P$. Then, $\sigma(f(Q))=\sigma(f)(\sigma(Q))=\sigma(f)(P)=f(P)=0$ for all $f\in\mathfrak{a}$ where $\sigma(f)=f$ because coefficients of f comes from k and $\sigma\in\textbf{Gal}\,[\overline{k}:k]$. ■

Let us now quickly discuss **projective algebraic sets**. We define a polynomial $f\in\overline{k}[x_0,x_1,\ldots,x_n]$ to be **homogeneous of degree** d if for any $\lambda\in\overline{k}$, we get

$$f(\lambda x_0,\lambda x_1,\ldots,\lambda x_n)=\lambda^d f(x_0,x_1,\ldots,x_n).$$

Let $\mathbb{P}^n(\overline{k})$ be the projective n-space over k. Let $S\subseteq\overline{k}[x_0,\ldots,x_n]$. A subset $V\subseteq\mathbb{P}^n(\overline{k})$ is called a projective algebraic set if

$$V=Z_h(S):=\{P\in\mathbb{P}^n(\overline{k})\mid f(P)=0\ \forall\text{ homogeneous }f\in S\}.$$

If $S\subseteq k[x_1,\ldots,x_n]$, then V is said to be defined over k, V/k. For an example, consider the homogeneous polynomial $f=a_0x_0+\cdots+a_nx_n\in k[x_0,\ldots,x_n]$. We have $Z_h(f)=\{P\in\mathbb{P}^n(\overline{k})\mid f(P)=0\}\subseteq\mathbb{P}^n(k)$, defining a projective algebraic set.

An ideal of $\overline{k}[x_0,\ldots,x_n]$ is said to be a **homogeneous ideal** if it is generated by homogeneous polynomials.

Remark 7.1.5. Remember that every polynomial in $\overline{k}[x_0,\ldots,x_n]$ can be written as a finite sum of homogeneous polynomials, and that a (proper) homogeneous ideal can be tested for prime by checking prime condition on homogeneous polynomials of $\overline{k}[x_0,\ldots,x_n]$. Finally, the analogue of Lemma 7.1.1 holds for projective algebraic sets, thus it gives Zariski topology to $\mathbb{P}^n(\overline{k})$.

Remember also that a topological space X is said to be **irreducible** if there are no two proper closed subspaces of X whose union is X.

Lemma 7.1.6. Let k be any field. $\mathbb{A}^1(\overline{k})$ and $\mathbb{P}^1(\overline{k})$ are irreducible in Zariski topology.

Proof. Any closed set in $\mathbb{A}^1(\overline{k})$ is of form $Z(\mathfrak{a})$ where $\mathfrak{a}\subseteq\overline{k}[x]$ is any ideal. We know that $\overline{k}[x]$ is a principal ideal domain. Hence, $\mathfrak{a}=\langle f(x)\rangle$ for some $f(x)\in\overline{k}[x]$. It follows that $Z(\langle f(x)\rangle)$ has only finitely many points, and thus every closed set of $\mathbb{A}^1(\overline{k})$ has only finitely many elements. But we know that algebraic closures always have infinitely many elements. This shows that there is no cover of $\mathbb{A}^1(\overline{k})$ by proper closed sets.

For $\mathbb{P}^1(\overline{k})$, we would like to use the same result proved above for affine case. To do this, first note that $\mathbb{P}^1(\overline{k}) = C \cup U$ where $C, U \subseteq \mathbb{P}^1(\overline{k})$ defined as $C = Z_h(\{x_0\})$ and $U = \mathbb{P}^1(\overline{k}) \setminus C$. Note we are working in $\overline{k}[x_0, x_1]$. C is closed while U is open in $\mathbb{P}^1(\overline{k})$. It follows that U is homeomorphic to $\mathbb{A}^1(\overline{k})$ in a natural way. But this means that any closed subspace of $\mathbb{P}^1(\overline{k})$ is also finite, which is what we needed (note that $Z_h(\{x_0\}) = \{[0,1]\}$ consists of only one point). ■

Finally, one defines an **affine algebraic variety** as a subset $V \subseteq \mathbb{A}^n(\overline{k})$ such that V is an irreducible subspace and closed. Similarly, one can define a **projective algebraic variety** as a subset $V \subseteq \mathbb{P}^n(\overline{k})$ which is closed and irreducible.

We know that given an algebraic set in $\mathbb{A}^n$ (or $\mathbb{P}^n$), we can obtain an ideal of $\overline{k}[x_1, \ldots, x_n]$ (or $\overline{k}[x_0, \ldots, x_n]$). However, an algebraic variety is an algebraic set which is supposed to be irreducible. What does this *topological* statement means algebraically is the premise of the following result. Remember that, intuitively speaking, the notion of prime elements in algebra is similar to that of irreducibility of spaces.

Proposition 7.1.7. Let k be a (perfect) field and consider the affine n-space $\mathbb{A}^n(\overline{k})$ over it. Let $V \subset \mathbb{A}^n(\overline{k})$. Then, V is affine algebraic variety if and only if $I(V) \subset \overline{k}[x_1, \ldots, x_n]$ is a prime ideal.
Exactly same result is true for projective spaces as well.

Proof. We will only show for affine case, the projective one follows by same arguments for affine case but focusing only on homogeneous polynomials.
(L $\implies$ R) Let $V \subset \mathbb{A}^n(\overline{k})$ be a variety. So $V = Z(S)$ for some $S \subset \overline{k}[x_1, \ldots, x_n]$. Let $fg \in I(V)$ for two $f, g \in \overline{k}[x_1, \ldots, x_n]$. Then we see that $Z(fg) = Z(f) \cup Z(g) \supset V$. Now $Z(f) \cap V$ and $Z(g) \cap V$ gives two proper closed subspaces of V. Irreducibility of V implies that we can consider $Z(f) \cap V = V$, so $Z(f) \supseteq V$. This shows that $f \in I(V)$.
(R $\implies$ L) Let $I(V)$ be prime. We wish to show V is a variety. Suppose V is not a variety. Then it should be reducible. Thus $V_1, V_2 \subset V$ are two closed subsets with $V_1 \cup V_2 = V$. Then $I(V_1), I(V_2) \supseteq I(V)$. Since V_1, V_2 are proper, therefore taking $f \in I(V_1) \setminus I(V)$ and $g \in I(V_2) \setminus I(V)$ gives $fg \in I(V)$, a contradiction. ■

A polynomial $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ is said to be **absolutely irreducible** if f is irreducible in $\overline{k}[x_1, \ldots, x_n]$. Similarly, an algebraic set $V/k \subset \mathbb{A}^n(\overline{k})$ over k is said to be absolutely irreducible if V is irreducible. Note that V/k is zero set of some polynomials from $k[x_1, \ldots, x_n]$, not from $\overline{k}[x_1, \ldots, x_n]$.

Example. Consider $x^2 + y^2 \in \mathbb{F}_3[x, y]$. We have it's zero-locus $V = Z(x^2 + y^2) \subset \mathbb{A}^2(\overline{\mathbb{F}_3})$. Since $x^2 + y^2$ is not irreducible in $\overline{\mathbb{F}_3}[x, y]$ because one can write $x^2 + y^2 = (x - ay)(x + ay)$ where $a \in \overline{\mathbb{F}_3}$ is an element such that $a^2 = 2$. By Proposition 7.1.7, V is not a variety as it is not irreducible. But note that $x^2 + y^2$ is irreducible in $\mathbb{F}_3[x, y]$. That is, even though V is not a variety, $I(V/\mathbb{F}_3)$ is a prime ideal. Hence analogue of Proposition 7.1.7 doesn't hold for V/k, it only holds in the algebraic closure.

The following lemma eases out the task of understanding projective varieties/spaces:

Lemma 7.1.8. Let k be a perfect field. Then the projective n-space $\mathbb{P}^n(\overline{k})$ has a finite open affine covering by $\mathbb{A}^n(\overline{k})$.

Proof. Consider the following $n + 1$ open subspaces of $\mathbb{P}^n(\overline{k})$:

$$U_i = \mathbb{P}^n(\overline{k}) \setminus Z(x_i)$$

for $i = 0, \ldots, n$. It is easy to see that $\bigcup_{i=0}^n U_i = \mathbb{P}^n$. One then argues that the following map

$$\theta_i : U_i \longrightarrow \mathbb{A}^n$$

$$[a_0, \ldots, a_i, \ldots, a_n] \longmapsto \left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i} \right)$$

establishes a homeomorphism, which is what we needed (note that $a_i \neq 0$ in above). ■

7.1.1 Dimension arguments

One defines an algebraic curve to be a variety of dimension 1. While the definition seems innocuous, it can be difficult for the uninitiated to figure out what should be the dimension of a variety by just the knowledge of it's generating polynomial equation. We devote this small section to dimension related arguments for varieties.

A **curve** in $\mathbb{A}^n(\overline{k})$ is a variety of dimension 1. Dimension of a variety here is defined in the usual way by looking at the topological dimension of that variety as a subspace of $\mathbb{A}^n(\overline{k})$, that is, the supremum of the lengths of proper chains of irreducible closed subspaces of your space. Hence, dimension of $\mathbb{A}^1(\overline{k})$ is 1.

Let us quickly draw some of the basic properties of dimension of topological spaces. First, any subspace $Y \subseteq X$ of a space X satisfies $\dim Y \leq \dim X$. Second, if a space X has an open cover $X = \bigcup_{i\in I} U_i$, then $\dim X = \sup_{i\in I} \dim U_i$. Lastly, if X is an irreducible space and $Y \subset X$ is a closed subspace, then $\dim X = \dim Y$ implies $X = Y$. One should keep these properties in mind for what follows.

The definition of curves above depend on a very topological definition of dimension. It is natural to ask thus whether we can characterize dimension of a variety to something more algebraic in nature. We have a notion of Krull dimension of rings[37], whose definition is also similar in essence to that of topological dimension, so one is justified to wonder whether topological dimension of a variety is related to Krull dimension of some ring attached to that variety. It turns out that this is true and this ring is our old (but of cosmic importance!) friend, the coordinate ring:

Definition 7.1.9. (**Coordinate Ring**) Let k be a (perfect) field and consider an algebraic set V in $\mathbb{A}^n(\overline{k})$. The coordinate ring of V is defined as the quotient ring, denoted $\overline{k}[V]$,

$$\overline{k}[V] := \frac{\overline{k}[x_1, \ldots, x_n]}{I(V)}.$$

Similarly, we define coordinate ring of $V \subseteq \mathbb{A}^n(\overline{k})$ over k naturally as

$$k[V] := \frac{k[x_1, \ldots, x_n]}{I(V/k)}.$$

We have already defined the notion of the dimension of topological spaces and also the notion of Krull dimension of commutative rings. We have also defined the height of a prime ideal. Suppose $[K : k]$ is a field extension. One defines the **transcendence degree** of the extension as the cardinality of the largest algebraically independent subset of K over k. In other words, the largest set $S = \{s_1, \ldots, s_n\} \subseteq K$ such that there is no non-zero polynomial f in $|S| = n$ amount of variables with coefficients in k with $f(s_1, \ldots, s_n) = 0$. For example, $[k(x_1, \ldots, x_n) : k]$ has transcendence degree of n over k. Transcendence degree of an extension is denoted as trdeg. We first state the following celebrated result from commutative algebra related to Krull dimension without the proof.

Theorem 17. Let k be a field and A be an integral domain which is a finitely generated k-algebra[38]. We then have the following two results:

[37] for a prime ideal $\mathfrak{p}$ of a ring R, one defines the height of $\mathfrak{p}$ as the supremum of the integers n as in the chains $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ where containments are proper and $\mathfrak{p}_i$ are other prime ideals of R. Then, the **Krull dimension** $\dim R$ of ring R is defined as the supremum of all heights of all prime ideals of R.

[38] this means that there is a collection of elements $\{a_1, \ldots, a_n\}$ such that every element of A is given by $f(a_1, \ldots, a_n)$ for $f \in k[x_1, \ldots, x_n]$. Another way of saying this is that A is isomorphic to $k[x_1, \ldots, x_n]/I$ for some ideal I. The latter equivalent definition shows the importance to our study of varieties and their coordinate rings.

1. The dimension of A is equal to the transcendence degree of fraction field of A over k:

$$\dim A = \text{trdeg}[A_{\langle 0\rangle} : k].$$

2. For any prime ideal $\mathfrak{p} \subset A$, we have the following formula:

$$\text{ht}\,(\mathfrak{p}) + \dim A/\mathfrak{p} = \dim A.$$

We also have the following results relating dimension to coordinate rings and calculating the dimension of $\mathbb{A}^n$ and $\mathbb{P}^n$.

Proposition 7.1.10. Let k be a (perfect) field and $\mathbb{A}^n(\overline{k})$ be the affine n-space over it. Let $V \subseteq \mathbb{A}^n(\overline{k})$ be a non-empty affine algebraic set. Then

$$\dim V = \dim \overline{k}[V]$$

where $\dim V$ is the topological dimension of V and $\dim \overline{k}[V]$ is the Krull dimension of coordinate ring.

Proof. Consider all irreducible closed subsets of V, i.e. subvarieties of V. In this set, form the longest chain of properly contained irreducible closed sets. By Proposition 7.1.7, reversing this chain gives us the longest chain of prime ideals containing $I(V)$. The latter is $\dim V$ and the former is $\dim \overline{k}[V]$, both of which thus becomes same. ■

This Proposition 7.1.10 a nice corollary:

Corollary 7.1.11. Let k be a perfect field. Then, $\dim \mathbb{A}^n = \dim \mathbb{P}^n = n$.

Proof. The affine case is easy to see after using Theorem 17, 1 and Proposition 7.1.10. In particular,

$$\begin{aligned}
\dim \mathbb{A}^n &= \dim \overline{k}[\mathbb{A}^n] \\
&= \dim \frac{\overline{k}[x_1, \ldots, x_n]}{I(\mathbb{A}^n)} \\
&= \dim \frac{\overline{k}[x_1, \ldots, x_n]}{\langle 0\rangle} \\
&= \dim \overline{k}[x_1, \ldots, x_n] \\
&= \text{trdeg}[\overline{k}(x_1, \ldots, x_n) : \overline{k}] \\
&= n.
\end{aligned}$$

For the projective case, we know that $\mathbb{P}^n(\overline{k})$ has an open cover by $\mathbb{A}^n(\overline{k})$. So, $\dim \mathbb{P}^n = \sup \dim \mathbb{A}^n = n$. ■

7.2 Sheaf of regular functions

For a given variety, one can have many many *nice* functions over it. One of the most important of them are those functions which around a point of the variety looks like some relatively simple fraction $p(x)/q(x)$. Such functions will be soon defined with more rigor and will be called regular functions. The nice thing about functions which are regular on a whole open subspace of variety is that they are *gluable*, meaning that one can glue a collection of such functions on different open subspaces which agrees on overlaps to form a new unique regular function on the whole of variety. This is just a reiteration of the sheaf condition, thus we see that regular functions arrange themselves into a sheaf over the given variety. We will see how one can extract a field out of such regular functions and how they are related to the familiar coordinate ring of the variety. In-fact, the whole discussion about sheaf of regular functions over a variety and structures derived henceforth from them can be treated as geometric interpretations of various localization of

coordinate ring of the given variety, as pointed towards by lemmas in Section 7.2.1.

So, let us first improve the type of varieties we will work with so the above discussion makes sense. We define **quasi-affine variety** $W \subseteq \mathbb{A}^n(\overline{k})$ to be an intersection of an affine variety $V \subseteq \mathbb{A}^n(\overline{k})$ with an open set $U \subseteq \mathbb{A}^n(\overline{k})$, that is, $W = V \cap U$.

Remark 7.2.1. Since any subspace of an irreducible space is irreducible and dense, so a quasi-affine variety is also irreducible.

One of the most important class of functions that we would like to have on a variety is the class of regular functions:

Definition 7.2.2. (**Regular functions at a point on a Variety**) Let k be a (perfect) field. Consider the affine n-space $\mathbb{A}^n(\overline{k})$ and let $V \subseteq \mathbb{A}^n(\overline{k})$ be a quasi-affine variety. Let $P \in V$ be a point of the variety. Then, a regular function at P is a function

$$f : V \subseteq \mathbb{A}^n(\overline{k}) \longrightarrow \overline{k}$$

such that there exists a neighborhood $N \subseteq V$ of point P over which the restricted $f|_N(x_1, \ldots, x_n) = p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ where $p, q \in \overline{k}[x_1, \ldots, x_n]$ are two polynomials with $q(Q) \neq 0 \; \forall Q \in N$. That is,

$$\begin{aligned} f|_N : N &\longrightarrow \overline{k} \\ Q &\longmapsto \frac{p(Q)}{q(Q)}. \end{aligned}$$

One defines a regular function for quasi-projective variety as follows: let $V \subseteq \mathbb{P}^n(\overline{k})$ be a quasi-projective variety. Let $P \in V$ be a point. A function

$$f : V \subseteq \mathbb{P}^n(\overline{k}) \longrightarrow \overline{k}$$

is said to be regular at P if f is regular in the quasi-affine variety $V \cap \mathbb{A}^n(\overline{k})$. In other words, if there exists open subset $N \subseteq V \cap \mathbb{A}^n(\overline{k})$ such that $f|_N(x_1, \ldots, x_n) = p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ with $p, q \in \overline{k}[x_1, \ldots, x_n]$ and $q \neq 0$ on N.

Remark 7.2.3. (**Structure Sheaf, Local Ring at a point & Function Field of a Variety**):-
Let k be a (perfect) field and V be a quasi-affine (or quasi-projective) algebraic variety. For any open subspace $U \subseteq V$ of variety V, we can define the collection of regular functions which is regular at each point of U. Let us denote this set by $\mathscr{O}_V(U)$. We see that for two regular functions $f, g \in \mathscr{O}_V(U)$, we can define $f + g$ and $f \cdot g$ by pointwise operations induced from $\overline{k}$. This makes $\mathscr{O}_V(U)$ a $\overline{k}$-algebra. Moreover, for an inclusion of open subspaces $W \subseteq U$ of V, we see that we get a map in the other direction

$$\begin{aligned} \mathscr{O}_V(U) &\longrightarrow \mathscr{O}_V(W) \\ f &\longmapsto f|_W \end{aligned}$$

which is indeed a $\overline{k}$-algebra homomorphism. In particular, we get a presheaf of $\overline{k}$-algebras, $\mathscr{O}_V$:

$$\mathscr{O}_V(-) : O(V)^{\mathrm{op}} \longrightarrow \overline{k}\mathbf{Alg}.$$

But one may notice that we have not used the *local* characteristic of regular functions in the above discussion. In-fact, it can be seen that this presheaf follows the sheaf condition because of it being locally constant to a rational function; $\mathscr{O}_V$ is a sheaf of $\overline{k}$-algebras. This sheaf is called the **sheaf of regular functions of a variety**. Note that a $f \in \mathscr{O}_V(U)$ is by definition regular at each point of U, this means (by irreducibility

of V) that at each point of U, f looks like the same rational fraction $p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$.

For every sheaf on a space, one can form it's stalk at each point, which is formed by collection of all germs at that point. We are assuming familiarity with sheaf theory so let us be a bit terse. More precisely, for a point $P \in V$, we first define the following relation on the set $\bigcup_{g \in \mathscr{O}_V(U)} \bigcup_{U \subseteq V, U \ni P} g$:

$$(f \in \mathscr{O}_V(U)) \sim (g \in \mathscr{O}_V(W)) \iff \exists \text{ nbhd. of } P,\, Y \subseteq U \cap W \text{ s.t. } f|_P = g|_P\,.$$

This is easily seen to be an equivalence relation. An equivalence class represented by $f \in \mathscr{O}_V(U)$ is denoted by $\mathrm{germ}_P f$ pronounced "germ of f at P". The collection of all such equivalence classes at P is denoted

$$\mathscr{O}_{V,P} := \{\mathrm{germ}_P f \mid f \in \mathscr{O}_V(U) \text{ for some open nbhd. of } P, U \subseteq V\}$$

and is called the **stalk of sheaf $\mathscr{O}_V$ at point** P. But we have more! This is not merely a set; under the following operations, $\mathscr{O}_{V,P}$ inherits a commutative ring structure with unity:

$$\mathrm{germ}_P f + \mathrm{germ}_P g := \mathrm{germ}_P f + g$$
$$\mathrm{germ}_P f \cdot \mathrm{germ}_P g := \mathrm{germ}_P f \cdot g.$$

These are well defined because of sheaf condition. Therefore, the stalk $\mathscr{O}_{V,P}$ at P is defined to be a **local ring of variety V at point** P. This ring $\mathscr{O}_{V,P}$ is not called local for aesthetic purposes, it is indeed a local ring in the sense that it has only one maximal ideal and it is given by

$$\mathfrak{m}_P := \{\mathrm{germ}_P f \mid f(P) = 0\},$$

that is, the germ of all those regular functions which become 0 at point P is the unique maximal ideal of ring $\mathscr{O}_{V,P}$. To see this, consider and $\mathrm{germ}_P f \in \mathscr{O}_{V,P}$ which is not 0 at P, i.e., $f(P) \neq 0$. Then we claim that $\mathrm{germ}_P f$ is a unit in $\mathscr{O}_{V,P}$. Indeed, if $N \subseteq \mathbb{A}^n(\overline{k})$ (or $\mathbb{P}^n(\overline{k})$) is a nbhd of P over which $f = p/q$ for two $p, q \in \overline{k}[x_1, \ldots, x_n]$. Note in particular $p(P)/q(P) \neq 0$, which means $p(P) \neq 0$. So if we define the function $g = q/p$ (which is well-defined at point P), then $\mathrm{germ}_P g \cdot \mathrm{germ}_P f = \mathrm{germ}_P 1$.

This is quite nice, we have defined an algebraic structure at each point of the variety. Moreover, each of these rings are local, and the unique maximal ideal is a very natural maximal ideal. However, from the definition of regular functions, we can contemplate yet another algebraic structure on the whole of variety V. Consider a regular function $f \in \mathscr{O}_V(U)$ on some open subspace $U \subseteq V$. We know that by definition f looks like a rational function $p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ when restricted to U. One can wonder whether there is some another regular function $g \in \mathscr{O}_V(W)$ on some other open subspace $W \subseteq V$ which also looks like $p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ on whole of W. Indeed, if we consider the following equivalence relation on the set $\bigcup_{U \subseteq V} \bigcup_{f \in \mathscr{O}_V(U)} f$

$$(U, f) \sim (W, g) \iff \exists \text{ open } Y \subseteq U \cap W \text{ s.t. } f|_Y = g|_Y$$

then it follows that an equivalence class $\overline{(U, f)}$ consists of all those regular functions which looks like the same rational function on their respective open subspace of V. Denote this collection of all equivalence classes as $\overline{k}_V$. This collection $\overline{k}_V$ not only forms a mere set, but forms a field. To see this, take any two $\overline{(U, f)}$ and $\overline{(W, g)}$. One sees that the following definitions are well-defined:

$$\overline{(U, f)} + \overline{(W, g)} := \overline{(U \cap W, f + g)}$$
$$\overline{(U, f)} \cdot \overline{(W, g)} := \overline{(U \cap W, f \cdot g)}.$$

This gives $\overline{k}_V$ a ring structure with zero element being $\overline{(U, 0)}$ and identity element being $\overline{(U, 1)}$. Finally, take any non-zero $\overline{(U, f)} \in \overline{k}_V$, since f is not zero on U, therefore $\overline{(U \setminus Z(f), 1/f)}$ forms the inverse of

$\overline{(U,f)}$. Hence, $\overline{k}_V$ is a field, called the **function field of variety** V.

One further notices that if $U \subseteq V$ is an open subspace of variety V, then the function field $\overline{k}_U$ is same as function field of the whole variety $\overline{k}_V$. One side of this is trivial to see, for the other, take any $(\overline{(W,g)}) \in \overline{k}_V$. Since any two open subspaces of V always intersect (because of irreducibility of V), therefore we have $(\overline{U \cap W, g}) \in \overline{k}_U$. But, $\overline{(U \cap W, g)} = \overline{(W,g)}$ by definition, therefore, $\overline{(W,g)} = (\overline{U \cap W, g}) \in \overline{k}_U$. On the hindsight, the fact that function field of a variety remains same if we are working even in some of it's subspace is quite an intriguing fact!

Now take some open subset $U \subseteq V$ of variety V. One can ask the following question on U: "*what all germs at any point of U has the property that it contains same guys as germs on other points of U?*". That is, we are asking about the elements in

$$\bigcap_{P \in U} \mathscr{O}_{V,P},$$

the intersection of all of the stalks in U. We claim the following for any open subset $U \subseteq V$:

$$\text{Claim : } \mathscr{O}_V(U) \cong \bigcap_{p \in U} \mathscr{O}_{V,P}.$$

To see this, take the mapping $f \in \mathscr{O}_V(U) \longmapsto \text{germ}_P f \in \bigcap_{P \in U} \mathscr{O}_{V,P}$. First of all, we need to show that this is well-defined. So take $f = g \in \mathscr{O}_V(U)$, then obviously $\text{germ}_P f = \text{germ}_P g$ for each $P \in U$ and hence this common germ is a member of $\bigcap_{P \in U} \mathscr{O}_{V,P}$. Next, take two equal germs $\text{germ}_P f, \text{germ}_P g \in \bigcap_{P \in U} \mathscr{O}_{V,P}$, where $f, g \in \mathscr{O}_V(U)$. Then because f and g looks same at each point of U, therefore they are same. Conversely, take any $\text{germ}_P f \in \bigcap_{P \in U} \mathscr{O}_V(U)$ where f may not be in $\mathscr{O}_V(U)$. Regularity of f gives us that f looks like $p(X)/q(X)$ on each point of U, hence the regular member $p(X)/q(X) \in \mathscr{O}_V(U)$ is taken by above map as $p(X)/q(X) \mapsto \text{germ}_P p(X)/q(X) = \text{germ}_P f \in \bigcap_{P \in U} \mathscr{O}_{V,P}$. This establishes the required isomorphism and hence the claim is correct.

Remark 7.2.4. (**Function field of Projective Varieties**) In the previous remark, we didn't mentioned much about the projective case. Indeed, by Lemma 7.1.8, we know that we can cover the entire projective space $\mathbb{P}^n(\overline{k})$ by affine n-spaces. Now take any projective variety $V \subseteq \mathbb{P}^n(\overline{k})$. Clearly, V intersects one of the members of the cover of $\mathbb{P}^n$ as guided by the Lemma 7.1.8, so this intersection looks like $V \cap U_i \cong V \cap \mathbb{A}^n(\overline{k})$ for some i, which looks like an affine variety. Also, by Remark 7.2.3, we know that function field of a variety doesn't change when we look at some open subspace of it. Now because $V \cap U_i \subseteq V$, thus, instead of giving the whole description of the function field of a projective variety, we reduce merely to the familiar case of function field of affine varieties. Hence, there is no ambiguity in projective case of function field; it is same as that of any of the affine subvariety contained in it.

7.2.1 Properties of $\mathscr{O}_V, \overline{k}[V]$ & $\overline{k}_V$

The previous remark introduces a lot of new terminology and new structures on varieties which clears a lot of mist surrounding them. So it is natural that we now study some easy properties derived from it.

Lemma 7.2.5. Let k be a field and $(V, \mathscr{O}_V)$ be a quasi-affine or a quasi-projective variety in $\mathbb{A}^n(\overline{k})$ or $\mathbb{P}^n(\overline{k})$. Then there is a bijection:

$$V \cong \text{mSpec } \overline{k}[V].$$

Proof. Consider the map:

$$V \longrightarrow \text{mSpec } \overline{k}[x_1, \ldots, x_n]$$
$$P \longrightarrow \mathfrak{m}_P := \{f \in \overline{k}[x_1, \ldots, x_n] \mid f(P) = 0\}.$$

First, $\mathfrak{m}_P$ is indeed a maximal ideal of $\overline{k}[x_1, \ldots, x_n]$ because $\mathfrak{m}_P = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ where $P = (a_1, \ldots, a_n)$ and we know that these are all the maximal ideals of $\overline{k}[x_1, \ldots, x_n]$. But note that $\mathfrak{m}_P \supseteq I(V)$. Therefore, quotienting out $I(V)$ gives the required correspondence between points and maximal ideals of coordinate ring $\overline{k}[V]$, which hence justifies the name given to $\overline{k}[V]$. ■

Lemma 7.2.6. Let k be a field and $(V, \mathscr{O}_V)$ be a quasi-affine variety in $\mathbb{A}^n(\overline{k})$. Let $P \in V$ be a point and consider the ideal $\mathfrak{m}_P = \{f \in \overline{k}[V] \mid f(P) = 0\}$ of $\overline{k}[V]$ corresponding to the point P. We then have an ring isomorphism:

$$\mathscr{O}_{V,P} \cong \overline{k}[V]_{\mathfrak{m}_P}.$$

Proof. Consider the map

$$\begin{aligned} \overline{k}[V]_{\mathfrak{m}_P} &\longrightarrow \mathscr{O}_{V,P} \\ \frac{f}{g} &\longmapsto \operatorname{germ}_P \frac{f}{g} \end{aligned}$$

where $f \in \overline{k}[V]$ and $g \in \overline{k}[V] \setminus \mathfrak{m}_P$. Well-definedness of this map follows easily. This map is injective because $\operatorname{germ}_P f/g = \operatorname{germ}_P f'/g'$ implies $\exists U \subseteq V$ which is a nbhd of P such that f/g and f'/g' are same when restricted to U, which means that f/g and f'/g' are same on whole space $\mathbb{A}^n(\overline{k})$ or $\mathbb{P}^n(\overline{k})$ (as two rational functions cannot be different at only finitely many points). Surjectivity is obvious; for any $\operatorname{germ}_P f \in \mathscr{O}_{V,P}$, since these are germs of regular functions, therefore $\exists g, h \in \overline{k}[x_1, \ldots, x_n]$ such that $\operatorname{germ}_P f = \operatorname{germ}_P g/h$ where $h(P) \neq 0$. ■

Lemma 7.2.7. Let k be a field and $(V, \mathscr{O}_V)$ be a quasi-affine variety in $\mathbb{A}^n(\overline{k})$. The function field $\overline{k}_V$ of V is the fraction field of coordinate ring $\overline{k}[V]$:

$$\overline{k}_V \cong \overline{k}[V]_{\langle 0 \rangle}.$$

Proof. Any element of function field $\overline{k}_V$ can be represented by the unique fraction $p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ where $q(x_1, \ldots, x_n) \neq 0$ on any point $P \in V$ and if $p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ is treated as zero whenever $p(x_1, \ldots, x_n)$ is zero on each point of V, i.e. $p \in I(V)$. This naturally identifies $p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ with an element of the fraction field $\overline{k}[V]_{\langle 0 \rangle}$. ■

Remark 7.2.8. It is trivial to observe that the Lemma 7.2.7 also holds for quasi-projective varieties in the light of Remark 7.2.4. Moreover then, one notes that for any quasi-affine or quasi projective variety V, we have:

$$\begin{aligned} (\mathscr{O}_{\mathcal{X},P})_{\langle 0 \rangle} &\cong (\overline{k}[V]_{\mathfrak{m}_P})_{\langle 0 \rangle} \\ &\cong \overline{k}[V]_{\langle 0 \rangle} \\ &\cong \overline{k}_V \end{aligned}$$

by Lemmas 7.2.6 and 7.2.7.

Remark 7.2.9. Motivated by Lemma 7.2.7, one further defines the **k-rational function field of** V, k_V as the field of fractions of the coordinate ring $k[V]$.

Lemma 7.2.10. Let k be a field and $(V, \mathscr{O}_V)$ be a quasi-affine variety in $\mathbb{A}^n(\overline{k})$. Then, we have a ring isomorphism:

$$\mathscr{O}_V(V) \cong \overline{k}[V].$$

Proof. First of all, $\overline{k}[V] \subseteq \mathscr{O}_V(V)$ because any element $f \in \overline{k}[V]$ naturally gives a $\mathrm{germ}_P f$ which has elements for any $P \in V$, hence $\mathrm{germ}_P f \in \mathscr{O}_V(V)$. Next, we see that $\mathscr{O}_V(V) = \bigcap_{P\in V} \mathscr{O}_{V,P} \cong \bigcap_{P\in V} \overline{k}[V]_{\mathfrak{m}_P}$, but we know that all maximal ideals of $\overline{k}[V]$ are of the form $\mathfrak{m}_P$ for some $P \in V$ by Lemma 7.2.6, therefore any element of $\bigcap_{P\in V} \overline{k}[V]_{\mathfrak{m}_P}$ is a fraction whose denominator is not contained in any maximal ideal of $\overline{k}[V]$. By Zorn's lemma, every non identity element is contained in some maximal ideal, hence only elements which are not contained in any maximal ideal are constants of $\overline{k}[V]$. This means $\bigcap_{P\in V} \overline{k}[V]_{\mathfrak{m}_P} = \overline{k}[V]$, hence $\mathscr{O}_V(V) \subseteq \overline{k}[V]$. ■

We also have the following two lemmas to help us find dimension of a given variety. An affine variety has dimension which is equal to the dimension of the local ring at any point of the variety:

Lemma 7.2.11. Let k be a field and let $(V, \mathscr{O}_V)$ be a quasi-affine variety in $\mathbb{A}^n(\overline{k})$. Then, we have the following equality for all $P \in V$:

$$\dim \mathscr{O}_{V,P} = \dim V$$

Proof. We know from Lemma 7.2.6 that $\mathscr{O}_{V,P} \cong \overline{k}[V]_{\mathfrak{m}_P}$. Therefore $\dim \mathscr{O}_{V,P} = \dim \overline{k}[V]_{\mathfrak{m}_P} = \mathrm{trdeg}[\overline{k}[V]_{\mathfrak{m}_P\langle 0\rangle} : \overline{k}] = \mathrm{trdeg}[\overline{k}[V]_{\langle 0\rangle} : \overline{k}] = \dim \overline{k}[V] = \dim V$, where we use Theorem 17, 1 and Proposition 7.1.10. ■

Note that the above lemma tells us that the dimension of a variety is locally encoded at each point. Another useful lemma relates dimension of a variety with trdeg of the function field:

Lemma 7.2.12. Let k be a field and $(V, \mathscr{O}_V)$ be an affine variety in $\mathbb{A}^n(\overline{k})$. Then,

$$\mathrm{trdeg}[\overline{k}_V : \overline{k}] = \dim V.$$

Proof. Since $\overline{k}_V \cong \overline{k}[V]_{\langle 0\rangle}$ by Lemma 7.2.7 and $\mathrm{trdeg}[\overline{k}[V]_{\langle 0\rangle} : \overline{k}] = \dim \overline{k}[V] = \dim V$ by Proposition 7.1.10 and Theorem 17, 1, we get the result. ■

Remark 7.2.13. Consider the function field $\overline{k}_V$ of variety V. Lemma 7.2.12 showed why we are calling $\overline{k}_V$ a *function field* of V in the first place; it tells us that as long as $\dim V \geq 1$, there is an element $\alpha \in \overline{k}_V$ which is not a root of any polynomial in $\overline{k}[x]$.

7.3 Morphism of varieties & $\mathbf{Var}_k$

Our next task is to define morphisms between two varieties. Since varieties are themselves a topological space, so this map has to be topologically continuous. But a variety is not only a topological space, it is a locally ringed space, that is, it has a sheaf of rings defined on it's open subspaces and the stalk at each point forms a local ring. Somehow, the notion of morphism between two varieties must also preserve these regular functions in an appropriate way. The following definition suggests how this might be done.

Definition 7.3.1. (**Morphism of Varieties**) Let $(V, \mathscr{O}_V)$ and $(W, \mathscr{O}_W)$ be two quasi-varieties in $\mathbb{A}^n(\overline{k})$ or $\mathbb{P}^n(\overline{k})$. A map $(\varphi, \varphi^\sharp) : (V, \mathscr{O}_V) \longrightarrow (W, \mathscr{O}_W)$ is a morphism of varieties if the following conditions are satisfied:

1. $\varphi : V \longrightarrow W$ is a topologically continuous map,
2. $\varphi^\sharp : \mathscr{O}_W \longrightarrow \varphi_* \mathscr{O}_V$ is a sheaf morphism which is defined as follows. Take any open subspace $U \subseteq W$:

$$\begin{aligned} \varphi^\sharp_U : \mathscr{O}_W(U) &\longrightarrow \varphi_* \mathscr{O}_V(U) := \mathscr{O}_V(\varphi^{-1}(U)) \\ f &\longmapsto \varphi^\sharp_U(f) := f \circ \varphi. \end{aligned}$$

The map $\varphi^\sharp_U$ is well-defined because if f is regular at each point of $U \subseteq W$, then $f \circ \varphi$ is regular at each point of $\varphi^{-1}(U) \subseteq V$ by the same rational fraction as f. Since $\varphi^\sharp$ is defined completely by the map φ alone, so one doesn't write all the time $\varphi^\sharp$ as some differently defined sheaf morphism (as far as varieties are concerned).

Note that the above definition transforms a regular map on some open subspace $U \subseteq W$ to a regular map on $\varphi^{-1}(U) \subseteq V$, hence qualifying itself to be called a *regular maps preserving function*, which is what we wanted to define. The map of sheaves $\varphi^\sharp$ as above defines a local homomorphism at each point of V:

Lemma 7.3.2. Let $(V, \mathscr{O}_V)$ and $(W, \mathscr{O}_W)$ be two quasi-varieties in $\mathbb{A}^n(\overline{k})$ or $\mathbb{P}^n(\overline{k})$ and let $(\varphi, \varphi^\sharp) : (V, \mathscr{O}_V) \longrightarrow (W, \mathscr{O}_W)$ be a morphism of varieties. For each $P \in V$, the map between stalks/local rings

$$\begin{aligned} \varphi^\sharp_P : \mathscr{O}_{W,\varphi(P)} &\longrightarrow \mathscr{O}_{V,P} \\ \mathrm{germ}_{\varphi(P)} f &\longmapsto \mathrm{germ}_P \varphi^\sharp_U(f) \end{aligned}$$

where $f \in \mathscr{O}_W(U)$ for some open $U \subseteq W$, is a local homomorphism of local rings.

Proof. We first show that this is well-defined. Let $\mathrm{germ}_{\varphi(P)} f = \mathrm{germ}_{\varphi(P)} g$ where $f \in \mathscr{O}_W(U), g \in \mathscr{O}_W(Y)$. Hence f and g are same in some open $Z \subseteq U \cap Y$. Now, $\varphi^\sharp_U(f) \in \mathscr{O}_V(\varphi^{-1}(U))$ and $\varphi^\sharp_Y(g) \in \mathscr{O}_V(\varphi^{-1}(Y))$ also agree on the open subsets $\varphi^{-1}(Z) \subseteq \varphi(U)^{-1} \cap \varphi^{-1}(Y)$ because $\varphi^\sharp_U(f) = f \circ \varphi$ and $\varphi^\sharp_Y(g) = g \circ \varphi$. Next, we will show that $(\varphi^\sharp_P)^{-1}(\mathfrak{m}_P) = \mathfrak{m}_{\varphi(P)}$ where $\mathfrak{m}_P \subset \mathscr{O}_{V,P}$ and $\mathfrak{m}_{\varphi(P)} \subset \mathscr{O}_{W,\varphi(P)}$ are their respective unique maximal ideals. Indeed, if one takes $\mathrm{germ}_{\varphi(P)} f \in (\varphi^\sharp_P)^{-1}(\mathfrak{m}_P)$, then $\varphi^\sharp_P(\mathrm{germ}_{\varphi(P)} f) = \mathrm{germ}_P \varphi^\sharp_U(f) \in \mathfrak{m}_P$, therefore $\varphi^\sharp_U(f)(P) = (f \circ \varphi)(P) = 0$, which implies that $f(\varphi(P)) = 0$ and hence $\mathrm{germ}_{\varphi(P)} f \in \mathfrak{m}_{\varphi(P)}$. Conversely, take any $\mathrm{germ}_{\varphi(P)} f \in \mathfrak{m}_{\varphi(P)}$, then $f(\varphi(P)) = (f \circ \varphi)(P) = 0$, and so $\mathrm{germ}_P f \circ \varphi \in \mathfrak{m}_P$ which further means that $\mathrm{germ}_P \varphi^\sharp_U(f) = \varphi^\sharp_P(\mathrm{germ}_{\varphi(P)} f) \in \mathfrak{m}_P$ and so $\mathrm{germ}_{\varphi(P)} f \in (\varphi^\sharp_P)^{-1}(\mathfrak{m}_P)$. This proves that $\varphi^\sharp_P : \mathscr{O}_{W,\varphi(P)} \longrightarrow \mathscr{O}_{V,P}$ is a local homomorphism. ∎

Remark 7.3.3. The map $\varphi^\sharp_P : \mathscr{O}_{W,\varphi(P)} \longrightarrow \mathscr{O}_{V,P}$ defined in Lemma 7.3.2 is usually called the **comorphism** of the morphism $(\varphi, \varphi^\sharp) : (V, \mathscr{O}_V) \longrightarrow (W, \mathscr{O}_W)$ between varieties.

In-fact, we will use the observation in the above lemma in order to motivate the definition of an *affine scheme*.

7.3.1 Properties of $(\varphi, \varphi^\sharp)$

We now state some main results regarding morphism of varieties:

Lemma 7.3.4. Consider a perfect field $\overline{k}$ and consider the affine line $\mathbb{A}^1(\overline{k})$ to be a variety itself. Let V be a quasi-affine or quasi-projective variety in $\mathbb{A}^n(\overline{k})$ or $\mathbb{P}^n(\overline{k})$ respectively. Then each global regular function $f \in \mathscr{O}_V(V)$ is a continuous morphism of varieties as in $V \longrightarrow \mathbb{A}^1(\overline{k})$.

Proof. We do for affine case, projective one follows exactly the same procedure. Since any closed set in $\mathbb{A}^1(\overline{k})$ is either $\mathbb{A}^1(\overline{k})$ or a finite collection of points, hence it is sufficient to check that $f^{-1}(a) \subseteq V$ is closed or not for any $a \in \mathbb{A}^1(\overline{k})$. Since $f \in \mathscr{O}_V(V)$, therefore $f(X) = p(X)/q(X)$ on V where $p, q \in \overline{k}[X]$ and $q \neq 0$ on V with $X = (x_1, \ldots, x_n)$. Hence for each $P \in f^{-1}(a)$, we have $p(P)/q(P) = a \iff p(P) - aq(P) = 0$. This means that $s(X) = p(X) - aq(X) \in \overline{k}[X]$ is such that $Z(s(X)) \cap V = f^{-1}(a)$. Hence $f^{-1}(a) \subseteq V$ is closed, proving that f is continuous. ■

The following proposition characterizes morphisms of varieties in affine space:

Proposition 7.3.5. Let k be a perfect field. Suppose we have two varieties $(V, \mathscr{O}_V) \subseteq \mathbb{A}^n(\overline{k})$ or $\mathbb{P}^n(\overline{k})$ and $(W, \mathscr{O}_W) \subseteq \mathbb{A}^m(\overline{k})$ and a function $\varphi : V \longrightarrow W$. Then, φ is a morphism of varieties if and only if $\pi_i \circ \varphi : V \longrightarrow \mathbb{A}^1(\overline{k})$ are global regular functions in $\mathscr{O}_V(V)$ for each $i = 1, \ldots, m$, where $\pi_i : \mathbb{A}^m(\overline{k}) \longrightarrow \mathbb{A}^1(\overline{k})$ are coordinate projection maps.

Proof. (L $\implies$ R) It is enough to show that $\pi_i : W \to \mathbb{A}^1(\overline{k})$ is in $\mathscr{O}_W(W)$ as φ is given to be a morphism of varieties. This follows easily because $\pi_i = x_i$ as a function where $x_i \in \overline{k}[x_1, \ldots, x_m]$, and hence $\pi_i \in \mathscr{O}_W(W)$ as it is rational at each point of W.
(R $\implies$ L) We are given that $\pi_i \circ \varphi : V \to \mathbb{A}^1(\overline{k})$ is continuous for each i, therefore $\varphi : V \to W$ is continuous as well. Next, to see φ takes regular functions to regular functions, take any open $U \subseteq W$ and consider the map

$$\begin{aligned} \varphi_U^\sharp : \mathscr{O}_W(U) &\longrightarrow \mathscr{O}_V(\varphi^{-1}(U)) \\ f &\longmapsto f \circ \varphi. \end{aligned}$$

We need to show that $f \circ \varphi$ is also regular on $\varphi^{-1}(U)$. This is trivial to see. ■

In the above, we have defined what is a variety and what is a morphism between varieties. The next obvious step would be to realize the category which they arrange themselves into.

Definition 7.3.6. (**Category of Varieties**) Let k be a perfect field. The category of varieties and morphisms of varieties is denoted by $\mathbf{Var}_k$ and it consists of

- objects which are varieties $(V, \mathscr{O}_V)$, quasi-affine or quasi-projective,
- arrows which are morphisms of varieties $(\varphi, \varphi^\sharp) : (V, \mathscr{O}_V) \longrightarrow (W, \mathscr{O}_W)$.

With this, we obtain the first equivalence between *geometry* and *algebra*:

Proposition 7.3.7. Let k be a perfect field and let V be any affine or projective variety and W be an affine variety. We then have the following isomorphism:

$$\mathrm{Hom}_{\mathbf{Var}_{\overline{k}}}(V, W) \cong \mathrm{Hom}_{\overline{k}-\mathbf{Alg}}(\mathscr{O}_W(W), \mathscr{O}_V(V))$$

Proof. Consider the map

$$\begin{aligned} \Phi : \mathrm{Hom}_{\mathbf{Var}_{\overline{k}}}(V, W) &\longrightarrow \mathrm{Hom}_{\overline{k}-\mathbf{Alg}}(\mathscr{O}_W(W), \mathscr{O}_V(V)) \\ \varphi : V \to W &\longmapsto - \circ \varphi : \mathscr{O}_W(W) \to \mathscr{O}_V(V). \end{aligned}$$

We claim that Φ is an isomorphism. Well-definedness is easy to see. For injectivity, suppose two morphisms of varieties $\varphi, \phi : V \to W$ are given with the property that $\Phi(\varphi) = \Phi(\phi)$, that is, $- \circ \varphi = - \circ \phi$. Since W is an affine variety in, say $\mathbb{A}^n(\overline{k})$, we get by Proposition 7.3.5 that $\pi_i \circ \varphi = \pi_i \circ \phi$ in $\mathscr{O}_V(V)$ for all $i = 1, \ldots, n$ where $\pi_i : W \to \mathbb{A}^1(\overline{k})$ are in $\mathscr{O}_W(W)$. We hence get that $\varphi = \phi$ as each of their projections are same. Conversely, take any $\chi : \mathscr{O}_W(W) \to \mathscr{O}_V(V)$ which is a $\overline{k}$-algebra homomorphism. We wish to show that there is a variety morphism $\varphi : V \to W$ such that $\Phi(\varphi) = \chi$. The following is our candidate for φ:

$$\begin{aligned} \varphi : V &\longrightarrow W \\ P &\longmapsto \varphi(P) := (\chi(\pi_1)(P), \ldots, \chi(\pi_n)(P)) \end{aligned}$$

where $\pi_i : W \to \mathbb{A}^1(\overline{k})$ are projections in $\mathscr{O}_W(W)$. We first need to check whether this is indeed a variety morphism. Using Proposition 7.3.5, we reduce to checking whether $\pi_i \circ \varphi$ is global regular of V or not, where $\pi_i : W \to \mathbb{A}^1(\overline{k})$ are projections. For this, one notes that $\pi_i \circ \varphi = \chi(\pi_i)$ the latter of which is in $\mathscr{O}_V(V)$ by definition of χ, hence φ is a variety morphism. Lastly, we need to check whether for any $f \in \mathscr{O}_W(W)$, we have that $f \circ \varphi = \chi(f)$ or not. This is the place where we will use that fact that χ is a homomorphism of $\overline{k}$-algebras. In particular, using Lemma 7.2.10, we reduce to the assumption that $f \in \mathscr{O}_W(W)$ is a polynomial in $\overline{k}[W]$. It follows that $f \circ \varphi(P) = f(\varphi(P)) = f(\chi(\pi_1)(P), \ldots, \chi(\pi_n)(P)) = \chi(f(\pi_1(P), \ldots, \pi_n(P)))$. Hence $f \circ \varphi = \chi(f)$, which shows that Φ is surjective as well. This completes the proof. ■

Let us state some basic consequences of the above proposition when we let V, W be affine varieties:

Corollary 7.3.8. Let V and W be two affine varieties. Then, V and W are isomorphic if and only if their coordinate rings $\overline{k}[V]$ and $\overline{k}[W]$ are isomorphic.

Proof. Follows from Lemma 7.2.10 and Proposition 7.3.7. ■

Corollary 7.3.9. Let $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m$ be two affine varieties. Then, any morphism of varieties $\varphi : V \longrightarrow W$ is such that there exists polynomials $f_1, \ldots, f_m \in \overline{k}[x_1, \ldots, x_n]$ so that φ is expressed as

$$\begin{aligned} \varphi : V &\longrightarrow W \\ P &\longmapsto (f_1(P), f_2(P), \ldots, f_m(P)). \end{aligned}$$

Proof. By Lemma 7.2.10, we have $\mathscr{O}_V(V) = \overline{k}[V]$ and $\mathscr{O}_W(W) = \overline{k}[W]$. Consider the map $\tilde{\varphi} : \overline{k}[W] \longrightarrow \overline{k}[V]$ induced by φ using Proposition 7.3.7. Now, we define a morphism of varieties as given below:

$$\begin{aligned} V &\longrightarrow W \\ P &\longmapsto (\tilde{\varphi}(\bar{x}_1)(P), \ldots, \tilde{\varphi}(\bar{x}_m)(P)) \end{aligned}$$

where $\bar{x}_1, \ldots, \bar{x}_m \in \overline{k}[W]$ are respective classes. We claim that this map is same as φ. For this, take any $P \in V$ and note that $\varphi(P)$ is obviously same as the value that the above map gives us. ■

The following lemma tells us that a basic open set of an affine n-space $\mathbb{A}^n$ is actually an affine variety in one bigger dimension $\mathbb{A}^{n+1}$, which is very interesting (try to picture in your head for $n = 2$):

Lemma 7.3.10. Let k be a perfect field and let $f \in \overline{k}[x_1, \ldots, x_n]$ be an irreducible polynomial whose affine variety is denoted $V = Z(f) \subset \mathbb{A}^n$. Then, the open set $\mathbb{A}^n \setminus Z(f)$ is isomorphic[39] to $Z(x_{n+1}f - 1) \subset \mathbb{A}^{n+1}$:

$$\mathbb{A}^n(\overline{k}) \setminus Z(f) \cong Z(x_{n+1}f - 1).$$

[39] this is an isomorphism of varieties, not of sets!

Proof. Consider the following candidate for isomorphism:

$$\varphi : \mathbb{A}^n \setminus Z(f) \longrightarrow Z(x_{n+1}f - 1) \subset \mathbb{A}^{n+1}$$
$$P = (a_1, \ldots, a_n) \longmapsto (a_1, \ldots, a_n, 1/f(P)).$$

This is well-defined and establishes a bijection of sets. We just need to check whether it is a morphism of varieties or not. Consider it's inverse (so we can make domain a variety). This inverse is the following mapping $(a_1, \ldots, a_{n+1}) \longmapsto (a_1, \ldots, a_n)$. Using Proposition 7.3.5, we reduce to the case of checking whether each component of φ^{-1} is a global regular function of variety $Z(x_{n+1}f - 1)$ or not, but because these component functions are merely identity, so the result follows. ■

Suppose we are given the affine n-space over $\overline{k}$, $\mathbb{A}^n(\overline{k})$. For some prime $\mathfrak{p} \subseteq \overline{k}[x_1, \ldots, x_n]$, we get an affine variety $Z(\mathfrak{p})$ from Proposition 7.1.7, which is a closed subspace of $\mathbb{A}^n(\overline{k})$. From the Lemma 7.3.10, we see that the corresponding open subspace $\mathbb{A}^n(\overline{k}) \setminus Z(\mathfrak{p})$ is actually itself an affine variety (hence closed) in one higher dimension, $\mathbb{A}^{n+1}(\overline{k})$. One thus defines an **affine open set** of $\mathbb{A}^n(\overline{k})$ to be an open subspace which is itself an affine variety (like the one given by Lemma 7.3.10). We next see that every affine variety has a cover by open affine sets:

Proposition 7.3.11. Let k be a perfect field and $V \subseteq \mathbb{A}^n$ be an affine variety. Then there is an affine open cover of V.

Proof. For this, we have to show that for each $P \in V$ and for each neighborhood $U \subseteq V$ of P, there exists an affine open subset $W \subseteq U$ containing P. Take $P \in V$ and any neighborhood $U \subseteq V$ of P. Since V has a cover of quasi-affine varieties, so we reduce to the case when V is quasi-affine with $V = W \cap V'$ where W is some open subspace of $\mathbb{A}^n$ and V' is an affine variety. We can thus further reduce to the case when $U = V$. So we have an affine open subvariety $V \subseteq V'$ and $P \in V$. Consider $C = V' \setminus V$ and consider the ideals $I(C), I(P) \subseteq \overline{k}[x_1, \ldots, x_n]$. It is clear that $I(P)$ cannot contain $I(C)$, otherwise $P \in C$ which is not possible. So there exists $f \in I(C)$ such that $f \notin I(P)$. So $W = Z(f)$ is such that $V \setminus V \cap W$ is an open subspace of V containing P. By Lemma 7.3.10, it is affine in one higher dimension, hence giving us an affine open subspace W of V containing P, as required. ■

7.3.2 Duality between V and $\overline{k}_V$

We will next see that, for some certain classes of *nice* varieties, one has an isomorphism between the morphisms between such varieties and the corresponding field homomorphisms of their function fields. Note that we are here not restricting to affine varieties, like when we did in Proposition 7.3.7, but rather make a claim about any type of varieties.

For two varieties V and W, one can consider various refinements of the notion of maps between them, by using an equivalence relation on maps between V (some subspace thereof) and W, and then calling an equivalence class some special morphism of V and W. One such notion of maps between varieties that of rational maps. But before that, we need to introduce the following lemma:

Lemma 7.3.12. Let $\varphi, \psi : V \longrightarrow W$ be two morphisms of quasi-affine or quasi-projective varieties such that there exists open $U \subseteq V$ such that $\varphi|_U = \psi|_U$. Then, φ and ψ are same as morphism of varieties.

Proof. By Proposition 7.3.11, we reduce to V and W being affine varieties where $U \subseteq V$ is an open subset such that $\varphi|_U = \psi|_U$. Now, by Corollary 7.3.9, we can assume $\varphi(P) = (f_1(P), \ldots, f_m(P))$ and $\psi(P) = (g_1(P), \ldots, g_m(P))$ for $f_i, g_i \in \overline{k}[x_1, \ldots, x_n]$. Now, since $\varphi|_U = \psi|_U$, therefore $Y = Z(f_1 - g_1, \ldots, f_m - g_m) \subseteq W \subseteq \mathbb{A}^m(\overline{k})$ is exactly the image of φ and ψ on $U \subseteq V$. But Y is a closed set of W, therefore $\varphi^{-1}(Y) \subseteq V$ is closed. But, $\varphi^{-1}(Y) = U$, therefore U is additionally closed. Now, we know that the closure of U is V because of irreducibility, but $\overline{U} \subseteq U$ because U is also a closed set containing U. Therefore $V \subseteq U$ and so $V = U$, which is what we wanted to show. ■

Here's the actual definition:

Definition 7.3.13. (**Rational Map of Varieties**) Let k be a perfect field and let V, W be two varieties over $\overline{k}$ (quasi-affine or quasi-projective). Define a pair (U, φ) where $U \subseteq V$ is open and $\varphi : U \longrightarrow W$ is a morphism of varieties. Define a relation on $\bigcup_{\text{open } U \subseteq V, \varphi \in \text{Hom}_{\mathbf{Var}_{\overline{k}}}(U,W)} (U, \varphi)$ as follows:

$$(U, \varphi) \sim (W, \psi) \iff \varphi|_{U \cap W} = \psi|_{U \cap W}\,.$$

This is an equivalence relation, where reflexivity and symmetry is obvious and transitivity follows from the usual observation that any two open subspaces of irreducible space intersect and by Lemma 7.3.12. Each equivalence class of such morphisms of varieties is collectively called a rational map from V to W. The **domain** of a rational map φ from V to W is the union of all open $U \subseteq V$ such that there exists a morphism (U, ψ) in the class of φ, denoted dom φ. Since dom φ is an open subspace of V, dom φ is itself a variety and hence φ can be treated as a morphism of varieties as in dom $\varphi \longrightarrow W$. If the image $\varphi(\text{dom } \varphi) \subseteq W$ is dense, then the rational map φ is said to be **dominant**. Furthermore, for a rational map φ from V to W, if there exists an open subspace $U \subseteq V$ and an open subspace $Y \subseteq W$ such that φ establishes an isomorphism between U and Y, then φ is said to be a **birational** map and V and W are said to be **birationally equivalent**. Note that birational maps are always dominant rational maps.

Note the term *maps* in rational maps is used tersely as it may happen that no member of a class (U, φ) have any image for some point $P \in V$.
There is a simple characterization of a dominant rational map:

Lemma 7.3.14. Let V and W be two varieties (quasi-affine or quasi-projective). A rational map $\varphi :$ dom $\varphi \subseteq V \longrightarrow W$ is dominant if and only if for each (U, φ_U) in the class of φ, the image $\varphi_U(U) \subseteq W$ is dense.

Proof. Remember that in a topological space, $\overline{\bigcup_{i \in I} C_i} \supseteq \bigcup_{i \in I} \overline{C_i}$ for subsets C_i. This show the $R \implies L$ part. For the converse, suppose φ is a rational map from V to W and (U, φ_U) is a member of class of φ such that $\varphi_U(U) \subseteq W$ is not dense. Therefore $\overline{\varphi_U(U)} \subset W$ is a proper closed subset of W which additionally contains $\varphi_U(U)$. Therefore $\varphi^{-1}(\overline{\varphi_U}(U)) \subseteq U$ and is a closed subset of variety dom φ. Two cases now arise, if $\varphi^{-1}(\overline{\varphi_U}(U)) = U$ or $\varphi^{-1}(\overline{\varphi_U}(U)) =$ dom φ. In the former, we get that U is clopen subspace of dom φ, which cannot be the case as dom φ is a variety so $U =$ dom φ and thus $\varphi(U) = \varphi_U(U) = \varphi(\text{dom } \varphi)$, which makes $\varphi_U(U)$ dense, against the assumption. In the latter, it follows that $\overline{\varphi_U(U)} = \overline{\varphi(\text{dom } \varphi)}$ which further means that $\overline{\varphi_U(U)} = \overline{\varphi(\text{dom } \varphi)} = W$ which again contradicts the assumption that $\varphi_U(U)$ was not dense. This shows (U, φ_U) should always be dense. ■

We thus have the main theorem of this discussion, that establishes a duality between varieties and their function fields (this should be seen in conjunction with Proposition 7.3.7):

Theorem 18. Let V and W be two (quasi-affine or quasi-projective) varieties over $\overline{k}$. Denote $\mathbf{Var}_{\overline{k}}^{\text{DR}}$ to be the category with objects as varieties over $\overline{k}$ and arrows as dominant rational maps between them. Then we have the following bijection:

$$\text{Hom}_{\mathbf{Var}_{\overline{k}}^{\text{DR}}}(V, W) \cong \text{Hom}_{\overline{k}-\mathbf{Alg}}\left(\overline{k}_W, \overline{k}_V\right).$$

Proof. Construct the following candidate map:

$$\begin{aligned} \Phi : \text{Hom}_{\mathbf{Var}_{\overline{k}^{\text{DR}}}}(V, W) &\longrightarrow \text{Hom}_{\overline{k}-\mathbf{Alg}}\left(\overline{k}_W, \overline{k}_V\right) \\ [\varphi] : V \to W &\longmapsto \Phi([\varphi]) : \overline{k}_W \to \overline{k}_V \end{aligned}$$

where $\Phi([\varphi])$ maps as follows:

$$\begin{aligned}\Phi([\varphi]) : \overline{k}_W &\longrightarrow \overline{k}_V \\ \overline{(Y, g)} &\longmapsto \overline{(\varphi^{-1}(Y), g \circ \varphi)}.\end{aligned}$$

Let us now be a bit terse and state only the required results needed to complete the proof. First, we need to show that this mapping $\Phi([\varphi])$ is well-defined. This follows from density of Im φ, which shows $\varphi^{-1}(Y)$ is non-empty, and from the fact that $\varphi : \text{dom } \varphi \longrightarrow W$ is a variety morphism, so it preserves regular functions. Next, we need to show whether $\Phi([\varphi])$ is a $\overline{k}$-algebra homomorphism. This follows easily. Next we want to show that $\Phi(-)$ is an injective mapping. For that, suppose $\Phi(\varphi) = \Phi(\psi)$ for two dominant rational maps φ, ψ from V to W. By Proposition 7.3.11, we reduce to the case when V is affine. Now, if we track any element of $\overline{k}_W$, we see, in conjunction with Lemma 7.3.12, that for each regular function g of W, we get $g \circ \varphi = g \circ \psi$ as morphism of affine varieties dom $\varphi =$ dom $\psi \to \mathbb{A}^1(\overline{k})$. So if we let g be the coordinate projections, then we get the desired result that $\varphi = \psi$.
Lastly, we wish to show the $\Phi(-)$ is surjective as well. For this, let us first state a general and easy result : let X and Y be topological spaces and $f : X \to Y$ be continuous map with Im f being a proper subset of Y. If Im f is dense, then (Im $f)^\circ$ is non-empty. The proof of this follows easily from contradiction. We will need another result for the proof of surjectivity, which characterizes those variety morphisms which have dense images in lieu of Proposition 7.3.7: let V be a variety and W be an affine variety where $\varphi : V \to W$ is a variety morphism. Then, Im $\varphi \subseteq W$ is dense if and only if the map $- \circ \varphi : \mathscr{O}_W(W) \to \mathscr{O}_V(V)$ is injective. L $\implies$ R uses the former lemma by looking locally at the point of W outside of image.

Now, to show that Φ is surjective, we take any $\overline{k}$-algebra homomorphism $\chi : \overline{k}_W \longrightarrow \overline{k}_V$. We wish to show that there is a dominant rational map φ from V to W such that

$$\chi(\overline{(-_1, -_2)}) = \overline{(\varphi^{-1}(-_1), -_2 \circ \varphi)}.$$

We first specify the domain of this dominant rational map. First, by Proposition 7.3.11, we reduce to the case when W is affine. Furthermore, by Lemma 7.2.7, we can write χ as follows:

$$\chi : \overline{k}[W]_{\langle 0 \rangle} \longrightarrow \overline{k}_V.$$

We then isolate the following m elements of $\overline{k}_V$, where $W \subseteq \mathbb{A}^m$:

$$\begin{aligned}\chi(x_1) &= \overline{(U_1, f_1)} \\ \vdots &= \vdots \\ \chi(x_m) &= \overline{(U_m, f_m)}.\end{aligned}$$

Now write $U = \bigcap_{i=1}^m U_i$, which is open in V. Next, we obtain a map:

$$\begin{aligned}\tilde{\chi} : \overline{k}[W] &\longrightarrow \mathscr{O}_V(U) \\ \sum_i a_i X^i &\longmapsto \sum_i a_i \chi(X^i)\end{aligned}$$

where $X = (x_1, \ldots, x_m)$ and $X^i = (x_1^{i_1}, \ldots, x_m^{i_m})$. This is a $\overline{k}$-algebra homomorphism. Now since a k-algebra homomorphism of fields is also a field homomorphism, and we know that the latter is always injective, therefore χ is injective and so $\tilde{\chi}$ is also injective. Further, by the above lemma in this proof, we see that the map $\varphi : U \longrightarrow W$ which $\tilde{\chi}$ induces via Proposition 7.3.7 has a dense image. Hence φ is a dominant rational map from $U \subset V$ to W whose image under Φ gives back χ. So Φ is also surjective, as was needed to complete the proof. ■

One derives the following two very important corollaries out of this:

Corollary 7.3.15. Let V and W be two varieties over $\overline{k}$ and let φ be a rational map from V to W. Then φ is a birational map if and only if the function fields $\overline{k}_V$ and $\overline{k}_W$ are isomorphic as $\overline{k}$-algebras.

Proof. Trivially follows from Theorem 18. ■

The main corollary is as follows, which characterizes curves:

Corollary 7.3.16. Let V be a variety of dimension 1, that is a curve, over $\overline{k}$. Then V is birationally equivalent to a curve in $\mathbb{A}^2(\overline{k})$, that is, a plane curve. ■

8 Concise overview of algebraic curves

We very tersely review the basic theory of curves in this section. It is this section in which the discussion of function fields and valuation rings of previous sections (Section 6.2) will come into play and will help us in understanding this rich piece of mathematics. First of all, an example of an affine algebraic curve is $y^2 = x^3$ in a field whose characteristic is not equal to 2. Note that one infers that this is a variety of dimension 1 formally via Theorem 17 and Proposition 7.1.10. A curve over k means that a variety over k (polynomials coming from k not $\overline{k}$) which is of dimension 1. One denotes a curve over k as $\mathcal{X}/k$.

In our intuitive picture of curves, over the affine plane, a singularity occurs whenever the Jacobian matrix of the curve becomes non-invertible. One can define a similar notion for algebraic curves on this context. Let $\mathcal{X}/k$ be a curve defined in $\mathbb{A}^n(\overline{k})$. Further, by Hilbert's basis theorem, let $f_1, \ldots, f_m \in \overline{k}[x_1, \ldots, x_n]$ be the basis polynomials for $I(\mathcal{X})$. Then $\mathcal{X}$ is **non-singular/smooth** at a point $P \in \mathcal{X}$ if the Jacobian $m \times n$ matrix of $\mathcal{X}$ at P:

$$\begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \cdots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}\Bigg|_P$$

has rank $n-1$. Taking for example curve $\mathcal{X} : y^2 - x^3$ in $\mathbb{A}^2(\mathbb{C})$, we see that the Jacobian matrix at any P is a 1×2 vector given as

$$\begin{bmatrix} -3x^2 & 2y^1 \end{bmatrix}\Big|_P .$$

If we take $P = (0,0) \in \mathcal{X}$, then the Jacobian at P is the zero vector, which has rank 0, which is less than 1, so the point $P = (0,0)$ corresponds to a singularity of $\mathcal{X}$, which makes sense as this curve $\mathcal{X}$ is the well-known cusp, which has an interesting singularity at $(0,0)$.

8.1 Smoothness, stalks & DVRs

Before we say anything, let us look at the main result which sets the stone for what's to come:

Theorem 19. Let k be a perfect field and $\mathcal{X}/k$ be an affine curve over k. Then, $\mathcal{X}$ is smooth at point $P \in \mathcal{X}$ if and only if the local ring at P, $\mathscr{O}_{\mathcal{X},P}$, is a discrete valuation ring.

Proof. We would like to reduce the problem to the characterization made in Lemma 6.2.16, because we have that the Jacobian matrix at P has rank $n-1$ for $\mathcal{X}$ and so that remaining one dimension should intuitively correspond to the dimension of $\mathfrak{m}/\mathfrak{m}^2$. For this, first note that $\mathscr{O}_{\mathcal{X},P} \cong \overline{k}[\mathcal{X}]_{\mathfrak{m}_P}$ where $\mathfrak{m}_P = \{f \in \overline{k}[\mathcal{X}] \mid f(P) = 0\}$, from Lemma 7.2.6. Obviously, the ring $\overline{k}[\mathcal{X}]_{\mathfrak{m}_P}$ is local, with the maximal ideal being $\mathfrak{m} = \mathfrak{m}_P \overline{k}[\mathcal{X}]_{\mathfrak{m}_P} \subset \overline{k}[\mathcal{X}]_{\mathfrak{m}_P}$. Denote $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(\overline{k})$ and let $A_P \subset \overline{k}[x_1, \ldots, x_n]$ be the maximal ideal given by $A_P = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Now, it can be seen (but we won't show) that the following map of $\overline{k}$-vector spaces:

$$\begin{aligned} \theta : \overline{k}[x_1, \ldots, x_n] &\longrightarrow \mathbb{A}^n(\overline{k}) \\ f &\longmapsto \left(\frac{\partial f}{\partial x_1}(P), \ldots, \frac{\partial f}{\partial x_n}(P) \right) \end{aligned}$$

restricts on A_P/A_P^2 to establish an isomorphism of $\overline{k}$-vector spaces:

$$\frac{A_P}{A_P^2} \cong \mathbb{A}^n(\overline{k}).$$

Now, let the Jacobian of $\mathcal{X}$ be denoted by J. It's a linear transform on $\mathbb{A}^n(\overline{k}) \cong A_P/A_P^2$, whose kernel space can be seen to be isomorphic to exactly $\mathfrak{m}/\mathfrak{m}^2$ (requires considerable work to see, but let us be terse). Now, $\overline{k}[x_1, \ldots, x_n]$ is Noetherian, hence so is it's quotients and localizations. In particular, $\overline{k}[\mathcal{X}]_{\mathfrak{m}_P} \cong \mathscr{O}_{\mathcal{X},P}$ is Noetherian of dimension 1. Thus, by Lemma 6.2.16 and rank-nullity, we conclude. ■

This theorem tells us that one may only look at the local ring at a point of the curve in order to conclude whether that curve is smooth or not at that point. In-fact, this is essentially how most of the important results in this section will look like. In particular, we will study less the geometry of curves but rather see that it's study is completely equivalent to study of an object in algebra, the algebraic function field in one variable. Realizing this will be the major goal of this section, rather than developing any geometry over them, which can be done, but for our applications, we need the algebra side of it.

We have only defined so far the smooth *affine* curve. But motivated by Theorem 19, one can define the following analog in the projective case:

Definition 8.1.1. (**Projective Non-Singular Curve**) Let k be a perfect field and let $\mathcal{X}/k$ be a projective curve (a projective variety of dimension 1). Then $\mathcal{X}$ is said to be smooth/non-singular at $P \in \mathcal{X}$ if the local ring at P, $\mathscr{O}_{\mathcal{X},P}$, is a DVR. A projective curve which is non-singular/smooth at all points is called non-singular/smooth projective curve.

The following proposition is standard but tells us something which is of a very fundamental importance in our study of curves:

Proposition 8.1.2. Let k be a perfect field and let $\mathcal{X}/k$ be an affine or a projective curve. Then, the function field of algebraic curve $\mathcal{X}/k$, $\overline{k}_{\mathcal{X}}$, is an algebraic function field of one variable over $\overline{k}$.

Proof. Remember, the study of function field of projective varieties also reduces to that of the affine case by Remark 7.2.4. So hence assume $\mathcal{X}/k$ is an affine curve. By Lemma 7.2.12, we know that $\text{trdeg}[\overline{k}_{\mathcal{X}} : \overline{k}] = \dim \mathcal{X} = 1$. Now, we also know that $\overline{k}_{\mathcal{X}} \cong \overline{k}[\mathcal{X}]_{\langle 0 \rangle}$ by Lemma 7.2.7. So $\text{trdeg}[\overline{k}[\mathcal{X}]_{\langle 0 \rangle} : \overline{k}] = 1$ and there is a transcendental element in $\overline{k}[\mathcal{X}]_{\langle 0 \rangle}$ over $\overline{k}$, let it be called $\alpha \in \overline{k}[\mathcal{X}]_{\langle 0 \rangle}$. This means that $\overline{k}[\mathcal{X}]_{\langle 0 \rangle}$ is a finite extension of $\overline{k}(\alpha)$, otherwise one can see that $\text{trdeg}[\overline{k}_{\mathcal{X}} : \overline{k}]$ will be higher than 1.
We next need to see that the full constant field of $\overline{k}_{\mathcal{X}}$ is exactly $\overline{k}$. For that we need to show that every algebraic element in $[\overline{k}_{\mathcal{X}} : \overline{k}]$ is in $\overline{k}$. But since it is a standard result in algebraic geometry that the full constant field of an affine variety over $\overline{k}$ is $\overline{k}$ itself, and we omit it's proof. ■

Remark 8.1.3. Let k be a field and $\mathcal{X}/k$ be an algebraic curve. Let $P \in \mathcal{X}$ be a smooth point. We then know by Theorem 19 that $\mathscr{O}_{\mathcal{X},P}$ is a DVR. Thus one defines the local parameter of the DVR $\mathscr{O}_{\mathcal{X},P}$ to be the local parameter of the curve $\mathcal{X}$ at point P. One also have the following valuation on the fraction field of $\mathscr{O}_{\mathcal{X},P}$

$$\text{ord}\,(-) : (\mathscr{O}_{\mathcal{X},P})_{\langle 0 \rangle} \cong \overline{k}_V \longrightarrow \mathbb{Z}$$

(see Remark 7.2.8) as discussed earlier in Section 6.2.3. This discrete valuation is denoted by v_P, in order to emphasize that this valuation is on the fraction field of the local ring at the smooth point P, which is equivalent to a discrete valuation of the extension $[\overline{k}_V : \overline{k}]$. To conclude, for any given curve $\mathcal{X}/k$ and any smooth point $P \in \mathcal{X}$, the local ring $\mathscr{O}_{\mathcal{X},P}$ is a DVR and the natural valuation on it's fraction field, which in this case becomes the function field of the curve, is denoted by v_P:

$$v_P : \overline{k}_V \longrightarrow \mathbb{Z}$$

and thus we obtain a discrete valuation of the field extension $[\overline{k}_V : \overline{k}]$.

The above remark also connects the notation that we followed in the discussion of valuation rings in Section 6.2.1, and the next result solidifies it further, where we see that not only each point gives a DVR with fraction field the function field of the curve but we also see it's converse, that is, every DVR with a function field of a curve necessarily comes as local ring of a point. This in other words means that DVRs with fraction field the function field of a curve are essentially the actual points of the curve, which is needless to speak, a very striking result:

Theorem 20. Let k be a field and let $\mathcal{X}/k$ be a non-singular projective curve over k. We have the bijection of sets

$$\begin{aligned}\mathcal{X} &\xrightarrow{\cong} \{R \in \mathbf{CRing} \mid R \text{ is a DVR with } R_{\langle 0\rangle} \cong \overline{k}_{\mathcal{X}}\}\\ P &\longmapsto \mathscr{O}_{\mathcal{X},P}.\end{aligned}$$

Proof. The well-definedness is easy to see by the fact that stalks are uniquely determined by points. For injectivity, let $P = [a_0, \ldots, a_n], Q = [b_0, \ldots, b_n] \in \mathcal{X} \subset \mathbb{P}^n(\overline{k})$. We can also write $P = [a_0, \ldots, a_{n-1}, 1]$ and $Q = [b_0, \ldots, b_{n-1}, 1]$ where $a_0 \neq b_0$. Now, by Lemma 7.2.6, we see that the rational polynomial $1/(x_0/x_n - a_0) \notin \mathscr{O}_{\mathcal{X},P}$ while it is in $\mathscr{O}_{\mathcal{X},Q}$. This tells us that $\mathscr{O}_{\mathcal{X},P} \neq \mathscr{O}_{\mathcal{X},Q}$.
To see surjectivity, first note that if R is a DVR with $R_{\langle 0\rangle} = \overline{k}_{\mathcal{X}}$, then by Lemma 3.1.11 of [NX09], $\exists P \in \mathcal{X}$ such that $\mathscr{O}_{\mathcal{X},P} \subseteq R$ and the unique maximal ideal of $\mathscr{O}_{\mathcal{X},P}$ is contained in the unique (by Lemma 6.2.14) maximal ideal of R. We then conclude by Lemma 6.2.15. ∎

8.2 Galois action and the case of finite fields

In the starting of Section 7, we defined an action of the Galois group $\mathbf{Gal}\ [\overline{k} : k]$ on $\mathbb{A}^n(\overline{k})$ and $\mathbb{P}^n(\overline{k})$. We will now like to see how it actually turns out in the case of curves over finite fields, i.e. when $k = \mathbb{F}_q$. Let us first see that the following map endows $\overline{k}[x_1, \ldots, x_n] = \overline{k}[X]$ with the structure of a $\mathbf{Gal}\ [\overline{k} : k]$-set:

$$\begin{aligned}\mathbf{Gal}\ [\overline{k} : k] \times \overline{k}[X] &\longrightarrow \overline{k}[X]\\ (\sigma, \sum_{i=1}^{n} a_i X^i) &\longmapsto \sum_{i=1}^{n} \sigma(a_i) X^i.\end{aligned}$$

We now wish to define an action of Galois group on the function field of a curve. This latter aim can be achieved for arbitrary varieties. Indeed, the following lemma tells one how it can be achieved:

Lemma 8.2.1. Let k be a field and V/k be an affine variety. Then, the following map endows $\overline{k}_V$ with the structure of a $\mathbf{Gal}\ [\overline{k} : k]$-set:

$$\begin{aligned}\mathbf{Gal}\ [\overline{k} : k] \times \overline{k}_V &\longrightarrow \overline{k}_V\\ \left(\sigma, \frac{f(X)}{g(X)}\right) &\longmapsto \frac{\sigma(f(X))}{\sigma(g(X))}\end{aligned}$$

where $\sigma(h(X))$ for $h(X) \in \overline{k}[X]$ is defined term-by term as above.

Proof. We will use the Lemma 7.2.7 in this case and we thus freely identify $\overline{k}_V$ with $\overline{k}[V]_{\langle 0\rangle}$. In order to define a group action on $\overline{k}[V]_{\langle 0\rangle}$, we rather first define it on $\overline{k}[V]$, via the following map:

$$\begin{aligned}\mathbf{Gal}\ [\overline{k} : k] \times \overline{k}[V] &\longrightarrow \overline{k}[V]\\ (\sigma, f(X)) &\longmapsto \sigma(f(X))\end{aligned}$$

by acting on each coefficient. However, we need to see that this is indeed well-defined. For this, take any $f(X) - g(X) \in I(V)$, so that $f(X) = g(X)$ in $\overline{k}[V]$. In order to do this, we need to show $\sigma(f(X)) = \sigma(g(X))$ in $\overline{k}[V]$, or, $\sigma(f(X)) - \sigma(g(X))$ in $I(V)$ which is equivalent to showing that $\sigma(f(P)) = \sigma(g(P))$ for all

$P \in V$. With the help of Remark 7.1.3 and the fact that $P \in V$ implies $\sigma(P) \in V$ for all $\sigma \in \mathbf{Gal}\,[\overline{k} : k]$, we see the following:

$$\begin{aligned}\sigma(f(P)) - \sigma(g(P)) &= \sigma(f(\sigma(\sigma^{-1}(P)))) - \sigma(g(\sigma(\sigma^{-1}(P))))\\ &= \sigma(f(\sigma^{-1}(P))) - \sigma(g(\sigma^{-1}(P)))\\ &= \sigma(f(\sigma^{-1}(P)) - g(\sigma^{-1}(P)))\\ &= \sigma(h(\sigma^{-1}(P)))\end{aligned}$$

where $h(X) \in I(V)$, and since $\sigma^{-1}(P) \in V$, we get that $h(\sigma^{-1}(P)) = 0$, which gives $\sigma(h(\sigma^{-1}(P))) = 0$, and thus $\sigma(f(P)) = \sigma(g(P))$ for all $P \in V$, which finally means that $\sigma(f(X)) = \sigma(g(X))$ in $\overline{k}[V]$.
We thus showed that $\overline{k}[V]$ is a $\mathbf{Gal}\,[\overline{k} : k]$-set, and it is thus easy to extend this group action to the fraction field of $\overline{k}[V]$. ■

We now see the most fundamental correspondence for the *nice* curves over finite fields and the places of their function fields:

Theorem 21. Let $\mathbb{F}_q$ be a finite field and consider a non-singular projective curve $\mathcal{X}/\mathbb{F}_q$. We then have the following *natural* bijection:

$$\begin{aligned}\{\mathbb{F}_q\text{-closed points of } \mathcal{X}\} &\longrightarrow \mathbf{Pl}\left([(\mathbb{F}_q)_{\mathcal{X}} : \mathbb{F}_q]\right)\\ \mathrm{Cl}\,(P) &\longmapsto v_P|_{(\mathbb{F}_q)_{\mathcal{X}}} : (\mathbb{F}_q)_{\mathcal{X}} \to \mathbb{Z}\end{aligned}$$

where $v_P : (\overline{\mathbb{F}_q})_{\mathcal{X}} \longrightarrow \mathbb{Z}$ is as defined in Remark 8.1.3. Furthermore,

$$\deg \mathrm{Cl}\,(P) = \deg v_P|_{(\mathbb{F}_q)_{\mathcal{X}}}\,.$$

8.3 The fundamental equivalence

The main theorem of this section is introduced here and it brings to light the fundamental connection between non-singular projective curves over a field and the corresponding algebraic function field. Instead of giving a complete account of this, we rather begin in the middle and just show what's important. One is not so much interested in variety morphisms between curves, but rather rational maps between them because of Theorem 18.

Remark 8.3.1. A rational map of curves is always either constant or dominant. The main reason behind this is because of the lack of more dimensions in a curve; a curve is by definition of dimension 1. Anyways, to see the proof, suppose $\phi : \mathcal{X}_1 \to \mathcal{X}_2$ is a rational map which is not constant. Then there are more than one point in Im ϕ. Take any point $P \in \text{Im } \phi$. We have $\{P\} \subset \overline{\text{Im } \phi} \subseteq \mathcal{X}_2$. If $\overline{\text{Im } \phi} = \mathcal{X}_2$, then there is nothing to show. If not, then we have a chain of properly contained irreducible subsets of $\mathcal{X}_2$ as in:

$$\{P\} \subset \overline{\text{Im } \phi} \subset \mathcal{X}_2$$

which contradicts the fact that $\mathcal{X}_2$ is a curve and hence should have dimension 1. Hence, one need only concern him/her with dominant rational maps between curves. In fact, we could have replaced $\mathcal{X}_1$ with any variety and this result would had remained the same.

One defines two projective curves $\mathcal{X}_1/k$ and $\mathcal{X}_2/k$ to be **k-isomorphic** if the corresponding function fields $\overline{k}_{\mathcal{X}_1}$ is k-linearly isomorphic to $\overline{k}_{\mathcal{X}_2}$. We then have the main theorem:

Theorem 22. Let k be a perfect field. We then have the following *natural* equivalence between non-singular projective curves over k and algebraic function fields of one variable over k:

$$\begin{aligned} \theta : \mathbf{Var}_k^{nSPC} &\xrightarrow{\equiv} \mathbf{AFF}_k^1 \\ \mathcal{X}/k &\longmapsto k_{\mathcal{X}} \\ \mathcal{X}_1/k \to \mathcal{X}_2/k &\longmapsto k_{\mathcal{X}_2} \to k_{\mathcal{X}_1} \end{aligned}$$

where $\mathbf{Var}_k^{nSPC}$ is the category of non-singular projective curves over k with arrows as dominant rational maps between them and $\mathbf{AFF}_k^1$ is the category of algebraic function fields in one variable over k and arrows as k-algebra homomorphisms.

Remark 8.3.2. Let us end this section with a brief discussion on how should one think about DVRs and the places. First of all, there's the following bijection that we laid out earlier; for a non-singular projective curve $\mathcal{X}/k$, we have

$$\{\text{DVRs } R \text{ with } R_{\langle 0 \rangle} = \overline{k}_{\mathcal{X}}\} \cong \{\text{Points of } \mathcal{X}\}.$$

But why all the pain with DVRs and places and all? Firstly, let us talk *how* DVRs. A DVR R should be thought of as a collection of rational polynomials[40], along with a special irreducible polynomial $p(X)$ (not rational) which governs this collection as follows: every rational polynomial in this collection should either not contain this polynomial $p(X)$ in both numerator and denominator, or, only in numerator. This is the DVR with the local parameter $p(X)$. Note that if we consider the fraction field of this ring, then it will contain all kinds of rational polynomials which are possible without restrictions coming from position of $p(X)$. Now, as we know formally, the DVR R comes equipped with a unique normalized discrete valuation which will send a rational polynomial to the power of the $p(X)$ that it has; this can only be non-negative as our intuition suggests because $p(X)$ can only appear in numerator, not in denominator. This is the normalized discrete valuation corresponding to the DVR R. Now, let us try to think of the unique maximal

[40] we are considering rational polynomials because of the fact that most of the time we are interested in the function fields arising from a non-singular projective curve.

ideal $\mathfrak{m}$ of DVR R in this light. We know from our formal discussion that $\mathfrak{m}$ is principal and that the generating element is none other than $p(X)$ itself. What does this mean for the place that $\mathfrak{m}$ holds in R? This means that the ideal $\mathfrak{m}$ is the collection of all those rational polynomials of R for which there is atleast one factor of $p(X)$ is present in the numerator. This is what the formal statement that $\mathfrak{m}$ is all those elements with valuation greater than equal to 1 comes from. This hopefully gives a good intuition of DVRs and how to think of them.

Secondly, let us now try to argue about *why* DVRs. In the previous sections, we saw various properties of the structure sheaf and we also saw that the knowledge of the function field of a curve can be completely obtained from a single point of it, via the fraction field of the stalk at that point. The point, say P of $\mathcal{X}$, also gives you an irreducible polynomial in $\overline{k}[\mathcal{X}]$, which is $X - P$ (in compact notation, that is). This of-course leads to a maximal ideal in $\overline{k}[\mathcal{X}]$, denoted $\mathfrak{m}_P = \langle (X - P) \rangle$. Remember that all of this came just from description of a point of $\mathcal{X}$. Now, you see, the stalk at P is the collection of all germs at P, that is two different elements of stalk corresponds to two different functions, both of which look like a different rational polynomial *around* point P. But it is entirely possible that the stalk at a point may not have a particular rational polynomial; fraction field of the coordinate ring may not be equal to the stalk, the reason being that the point P can have various different rational polynomials which are zero at P, thus giving non-trivial elements to the maximal ideal of the local ring which is the stalk. But, the stalk has enough elements that as soon as we invert each non-zero element (considering the fraction field of stalk), we get the all rational polynomials (fraction field of coordinate ring, $\overline{k}[\mathcal{X}]_{\langle 0 \rangle}$). Now, we have a big field, called the function field of $\mathcal{X}$. This is big because the stalk of each point of the curve is contained in it as a subring. Hence, every DVR with fraction field equaling the function field is contained in the function field (so under the isomorphisms, every point is *essentially* contained in the function field via the stalks). Coming back to point P, we have $\mathfrak{m} = \langle X - P \rangle \subset \mathscr{O}_{\mathcal{X},P} \subset \overline{k}_{\mathcal{X}}$. Now, the valuation of the DVR $\mathscr{O}_{\mathcal{X},P}$ is just telling you the information that where does instance of $p(X)$ lies in each rational polynomial in $\overline{k}[\mathcal{X}]_{\langle 0 \rangle}$; does a given rational polynomial has $p(X)$ as a pole (valuation will be < 0), as a zero (valuation will be > 0) or nothing at all (valuation will be 0). Hence, the name "place" fits well with the intuitive understanding of it giving us the *place*, so to speak, of each rational polynomial with respect to a predefined polynomial $p(X)$. To summarize:
"*A DVR/place is just what you get naturally when you wish to consider the information that where does the irreducible polynomial defining a given point of the curve lies with respect to each rational polynomial over a curve.*"

8.4 Divisors

The notion of a divisor brings us closer to doing homological algebra over a variety/curve. Since our focus is on curves, so we will restrict all our attention only to divisors over a curve. Under the fundamental equivalences of Theorems 21 and 22, we can equivalently talk about divisors of an algebraic function field of one variable over k. We will follow the latter, but will make an effort to translate whatever results we might get into the former. We will be very brusque in our presentation in here and most of what will follow.

Definition 8.4.1. (**Divisor Group of a Function Field**) Let k be a perfect field and $[F : k]$ be an algebraic function field in one variable over k. Denote $\mathbf{Pl}([F : k])$ to be the set of places of the function field. Then, the divisor group of $[F : k]$ is defined to be the free abelian group generated by the set $\mathbf{Pl}([F : k])$:

$$\mathrm{Div}([F : k]) := \bigoplus_{P \in \mathbf{Pl}([F:k])} \mathbb{Z}.$$

Remark 8.4.2. By Theorem 21, one equivalently defines the *divisor group of a curve* $\mathcal{X}/\mathbb{F}_q$ to be the free group generated by the set of all closed points of $\mathcal{X}$.

One may want to compare the above definition by the definition of the zeroth singular chain group of a topological space. Anyways, with this definition one can now talk about particular kinds of divisors and can translate back various constructions to the level of elements of the function field. This latter remark will be helpful in the discussion and buildup to Riemann-Roch theorem.

There are more definitions in order. A divisor $D = (n_P)_{P \in \mathbf{Pl}([F:k])} \in \mathrm{Div}([F : k])$ is called **effective** if $n_P \geq 0$ for all places P of $[F : k]$. One denotes an effective divisor by writing $D \geq 0$. Now remember from the discussion in Section 6.2.1, and in particular Lemma 6.2.3 that every place has a unique normalized discrete valuation of $[F : k]$, denoted $v_P : F \to \mathbb{Z}$. As usual, the **support** of a divisor $D = (n_P)$ is the finite set of all those places $P \in \mathbf{Pl}([F : k])$ such that $n_P \neq 0$. Finally, the **degree** of a divisor $D = \sum_{P \in \mathbf{Pl}([F:k])} n_P P$ is the defined to be the sum of degree of each place P weighed by n_P:

$$\deg D = \sum_{P \in \mathbf{Pl}([F:k])} n_P \deg P$$

where $\deg P$ is as defined in Definition 6.2.9.

Let P be a place of $[F : k]$ and take a non-zero element $x \in F^*$. One calls the place P to be a **zero** of $x \in F^*$ if $v_P(x) > 0$ (i.e. if $x \in \mathfrak{m}_P$ by Lemma 6.2.5 & the observation that v_P is normalized) and P is called to be a **pole** of $x \in F^*$ if $v_P(x) < 0$ (i.e. $x \notin \mathcal{O}_P$ by Definition 6.2.4). One also denotes the set of all zeros and poles of $x \in F^*$ by $\mathcal{N}(x) \subseteq \mathbf{Pl}([F : k])$ and $\mathcal{P}(x) \subseteq \mathbf{Pl}([F : k])$, respectively.

Lemma 8.4.3. Let $[F : k]$ be a function field and let $x \in F^*$. Then, there are only finitely many poles and zeros of x, that is,

$$|\mathcal{P}(x)|, \ |\mathcal{N}(x)| < \infty$$

Proof. This is Corollary 3.3.2 of [NX09]. ∎

We need few more definitions to set the stage. Take $x \in F^*$. Above result tells us that it has finitely many poles and zeros. One is thus motivated to define following three divisors of $[F : k]$ using $x \in F^*$:

1. **Zero divisor of** x, denoted $(x)_0$ is:

$$(x)_0 := \sum_{P \in \mathcal{N}(x)} v_P(x)P.$$

2. **Pole divisor of** x, denoted $(x)_\infty$ is:

$$(x)_\infty := \sum_{P \in \mathcal{P}(x)} (-v_P(x))P.$$

3. **Principal divisor of** x, denoted $\operatorname{div}(x)$ is:

$$\operatorname{div}(x) := (x)_0 - (x)_\infty = \sum_{P \in \mathbf{Pl}([F:k])} v_P(x)P.$$

Since $\operatorname{div}(xy) = \sum_{P \in \mathbf{Pl}([F:k])} v_P(xy)P = \sum_{P \in \mathbf{Pl}([F:k])} (v_P(x) + v_P(y))P = \operatorname{div}(x) + \operatorname{div}(y)$, thus $\operatorname{div}(-) : F^* \longrightarrow \operatorname{Div}([F:k])$ is a group homomorphism.

8.5 The Riemann-Roch theorem

The highly celebrated Riemann-Roch theorem connects the complex analysis of compact Riemann surfaces to purely algebraic background via the concept of what is called the genus of a surface. Even though for our purposes, this won't be of much help, but this deep result is very much connected to the elliptic curves (which are *compact Riemann surfaces of genus 1*, as we will soon see), so we will look at it's brief treatment here. For more details, refer to Sections 3.4 to 3.6 of [NX09].

Our approach here will be algebraic, rather than analytic. We will reach the Riemann-Roch theorem in three steps. We will first learn about Riemann-Roch spaces, which is a particular subspace of F, treated as a k-vector space. Then we will learn about Riemann's theorem, which is the result which when improved gives us the Riemann-Roch theorem. Finally we will introduce concept of genus, adéles & Weil differentials, leading to the actual Riemann-Roch theorem and then provide a brief sketch of it's proof.

Definition 8.5.1. (**Riemann-Roch space**) Let $[F : k]$ be a function field and let $D \in \mathrm{Div}([F : k])$ be a divisor. Then, the k-vector space of all those elements $x \in F^*$ together with $0 \in F$ whose principal divisor becomes effective when added with D, is denoted $\mathcal{L}(D)$ and is called the Riemann-Roch space of divisor D. More formally:

$$\mathcal{L}(D) = \{x \in F^* \mid \mathrm{div}(x) + D \geq 0\} \cup \{0\}.$$

One denotes the dimension of $\mathcal{L}(D)$ over k as:

$$\ell(D) := \dim_k \mathcal{L}(D).$$

By the axioms of valuations, one can infer that $\mathcal{L}(D)$ is indeed a k-vector space.

Remark 8.5.2. Let us explain what the above definition is trying to say geometrically under the translation using Theorem 22. Note that one thinks of function field of a non-singular projective curve as the quotient field of coordinate ring in it's some affine subvariety (Remark 7.2.4). Thus a place is treated intuitively as a discrete valuation taking rational polynomials to integers. The principal divisor of a rational polynomial thus becomes simply a formal sum of places telling us which place is a pole and which is a zero and which is neither. The Riemann-Roch space of an arbitrary divisor D of the curve is the collection of those rational polynomials whose poles and zeros are *managed* by the divisor D nicely (it *accommodates* all the poles of the element and doesn't behave too badly with it's own set of poles). Why is this space important would be clearly visible soon.

The main reason why Riemann-Roch space is introduced is due to the importance of it's dimension $\ell(D)$, as specified by the following theorem, which is the starting point of Riemann-Roch theorem:

Theorem 23. (**Riemann's Theorem**) Let $[F : k]$ be a function field. Then, there exists a non-negative integer g such that,

$$\ell(D) \geq \deg D + 1 - g\ , \quad \forall D \in \mathrm{Div}([F : k]).$$

Proof. Section 3.5 of [NX09]. ■

We have few basic corollaries:

Corollary 8.5.3. Let $[F : k]$ be a function field and $G, D \in \mathrm{Div}([F : k])$. If $\ell(D) = \deg D + 1 - g$ and $G \geq D$, then $\ell(G) = \deg G + 1 - g$.

The following shows the uniqueness of non-negative integer g for a given function field:

Corollary 8.5.4. Let $[F : k]$ be a function field. There exists an integer r depending only on $[F : k]$ such that

$$\ell(D) = \deg D + 1 - g$$

for all $D \in \mathrm{Div}([F : k])$ with $\deg D \geq r$.

The above corollary justifies the following definition:

Definition 8.5.5. (**Genus of a Function Field**) Let $[F : k]$ be a function field. The non-negative integer g for which the Corollary 8.5.4 holds is called the genus of function field $[F : k]$. Similarly, for a non-singular projective curve $\mathcal{X}/k$, we define it's genus to be the genus of the function field $[k_{\mathcal{X}} : k]$.

A particularly simple example comes from the rational function field:

Example. Let $[k(x) : k]$ be a rational function field. We will find it's genus using Corollary 8.5.4. For this, take $r = 0$. Then, for every divisor $D \in \mathrm{Div}([k(x) : k])$ with $\deg D \geq 0$, we have $\ell(D) = \deg D + 1 - g$. We will first find all such D and then their $\ell(D)$. Now, a divisor with $\deg D \geq 0$ specifies no poles at any place and thus may only define zeroes at some finitely many places. Hence, such divisors are equivalent to nP_∞ for $n \geq 0$ and P_∞ being the infinite place. Therefore, if we now look at what it entails in the Riemann-Roch space (which actualizes the connection between the formal combination of places to those combinations coming from actual rational polynomials), we get that

$$\mathcal{L}(nP_\infty) = \left\{ \frac{f(x)}{g(x)} \in k(x) \mid g(x) = 1,\ f(x) \in k[x] \ \&\ \deg f(x) \leq n \right\}.$$

Obviously, $\ell(nP_\infty) = n+1$. Moreover, we know that $\deg P_\infty = \dim[\mathscr{O}_\infty/\mathfrak{m}_\infty : k] = 1$, therefore $n+1-g = n+1$ which implies $g = 0$, that is genus of rational function fields is zero. Converse is also true, that is, every function field of genus zero is a rational function field. But let us not prove that here as it requires results which we haven't developed here.

We now get a bit more close to Riemann-Roch theorem. Our main goal is to add more terms in Theorem 23 so that the inequality disappears. For this, we will observe that the inequality appears in the first place because there is a "missing dimension" of a subspace associated to a divisor which we haven't added, but we should, in order to get equality. So let us now develop the definitions which will lead us to this missing subspace. As it might have been observed starting from previous few sections, our goal is to develop definitions and state results than to develop their proofs.

Definition 8.5.6. (**Adéles**) Let $[F : k]$ be a function field. Any map of the form

$$\begin{aligned} \alpha : \mathbf{Pl}([F : k]) &\longrightarrow F \\ P &\longmapsto \alpha_P \end{aligned}$$

where $\alpha_P \in \mathscr{O}_P$, the valuation ring of place P, for almost all $P \in \mathbf{Pl}([F : k])$, is called an adéle of function field $[F : k]$. One may also define the set of all adéles of $[F : k]$ to be the restricted direct product:

$$\mathcal{A}_{[F:k]} := \prod_{P \in \mathbf{Pl}([F:k])}^{\times} F$$

where restricted here means that any element in the above has all but finitely many elements in their corresponding valuation rings. This set $\mathcal{A}_{[F:k]}$ is also called the **adéle space** of $[F : k]$. Clearly, the adéle space of a function field is a k-vectors space where the k-vector space structure is inherited from $\prod_{P \in \mathbf{Pl}([F:k])} F$.

For each element $x \in F$, one defines the adéle $(x)_{P \in \mathbf{Pl}([F:k])} \in \mathcal{A}_{[F:k]}$. It is indeed an adéle because the amount of places P at which it is not in $\mathscr{O}_P$ is the same set as that of the $\mathcal{P}(x)$, which is always finite by Corollary 3.3.2 of [NX09]. This adéle $(x) \in \mathcal{A}_{[F:k]}$ is therefore called the **principal adéle** of $x \in F$. Note that this gives us an embedding $F \longrightarrow \mathcal{A}_{[F:k]}$. Moreover, the valuations of any place P, $v_P : F \to \mathbb{Z} \cup \{\infty\}$ extends uniquely to a map $v_P : \mathcal{A}_{[F:k]} \to \mathbb{Z} \cup \{\infty\}$ which maps as $(\alpha_P)_{P \in \mathbf{Pl}([F:k])} \longmapsto v_P(\alpha_P)$. Note that it's image will be almost everywhere positive.

Associated to each divisor $D \in \mathrm{Div}([F:k])$, we can (and we will, you won't stop us!) a subspace of k-vector space $\mathcal{A}_{[F:k]}$ as below using the valuation of each place:

$$\mathcal{A}_{[F:k]}(D) := \{\alpha \in \mathcal{A}_{[F:k]} \mid v_P(\alpha) + v_P(D) \geq 0 \ \forall P \in \mathbf{Pl}([F:k])\}$$

which can be more explicitly be written as (if we write $D = \sum_{P \in \mathbf{Pl}(]F:k]} n_P P$):

$$\mathcal{A}_{[F:k]}(D) = \{\alpha = (\alpha_P)_{P \in \mathbf{Pl}([F:k])} \in \mathcal{A}_{[F:k]} \mid v_P(\alpha_P) + n_P \geq 0 \ \forall P \in \mathbf{Pl}([F:k])\}.$$

Next object that we need to define is that of a Weil differential. For this, we should first note that $\mathcal{A}_{[F:k]} + F$ is a subspace of k-vector space $\mathcal{A}_{[F:k]}$ because for any $(\alpha_P + x)_{P \in \mathbf{Pl}([F:k])} + (\beta_P + y)_{P \in \mathbf{Pl}([F:k])} \in \mathcal{A}_{[F:k]} + F$ and $x, y \in F$, we get that $(\alpha_P + x) + (\beta_P + y) = (\alpha_P + \beta_P + x + y)$ is again an element of $\mathcal{A}_{[F:k]} + F$ because $\alpha_P + \beta_P \in \mathscr{O}_P$ if both of them are.

Definition 8.5.7. (**Weil Differential**) Let $[F:k]$ be a function field. A Weil differential is a k-linear map

$$\omega : \mathcal{A}_{[F:k]} \longrightarrow k$$

such that $\exists D \in \mathrm{Div}([F:k])$ so that the map ω restricts on the subspace $\mathcal{A}_{[F:k]}(D) + F \subseteq \mathcal{A}_{[F:k]}$ (via the embedding $F \hookrightarrow \mathcal{A}_{[F:k]}$) to the zero map, that is,

$$\omega|_{\mathcal{A}_{[F:k]}(D)+F} = 0.$$

This means that $\forall (\alpha_P + x) \in \mathcal{A}_{[F:k](D)} + F$ where $x \in F$, we have $\omega((\alpha_P + x)) = 0$. We denote the set of all Weil differentials as $\Omega_{[F:k]}$. It is a k-vector space where addition is pointwise. One also defines the following obvious subspace of $\Omega_{[F:k]}$ for any divisor $D \in \mathrm{Div}([F:k])$:

$$\Omega_{[F:k]}(D) := \left\{\omega \in \Omega_{[F:k]} \mid \ \omega|_{\mathcal{A}_{[F:k]}(D)+F} = 0\right\},$$

that is, $\Omega_{[F:k]}(D)$ is that subspace of $\Omega_{[F:k]}$ where each Weil differential vanishes on the subspace $\mathcal{A}_{[F:k]}(D) + F$ of k-vector space $\mathcal{A}_{[F:k]}$.

Now, there is the following result which one yields from the above definitions, let us state it here itself. Let $\omega : \mathcal{A}_{[F:k]} \longrightarrow k$ in $\Omega_{[F:k]}$ be a non-zero Weil differential. We can attach a unique divisor to it. Call this divisor W. This divisor W will be obtained as follows; form the collection of all those divisors D in $\mathrm{Div}([F:k])$ such that $\omega|_{\mathcal{A}_{[F:k]}(D)+F} = 0$. This is a poset under $\leq$. The top element of this poset is exactly the required divisor W. This is the Lemma 3.6.11 of [NX09].

So for any Weil differential ω, we have a unique divisor W naturally attached to it via the above process. This calls for the following definition:

Definition 8.5.8. (**Canonical Divisor**) Let $[F:k]$ be a function field and let $\omega \in \Omega_{[F:k]}$ be any Weil differential. Then, the divisor $W \in \mathrm{Div}([F:k])$ such that $\omega|_{\mathcal{A}_{[F:k]}(W)+F} = 0$ and $\forall D \leq W$, $\omega|_{\mathcal{A}_{[F:k]}(D)+F} = 0$, is called a canonical divisor of ω. This divisor W is also denoted by (ω). One then also calls a divisor W which is canonical for some $\omega \in \Omega_{[F:k]}$ as a canonical divisor of F.

Remark 8.5.9. The subspace of $\Omega_{[F:k]}$ given by divisor D, $\Omega_{[F:k]}(D)$ can alternatively be given as

$$\begin{aligned}\Omega_{[F:k]}(D) &= \{\omega \in \Omega_{[F:k]} \mid \omega|_{\mathcal{A}_{[F:k]}(D)+F} = 0\} \\ &= \{\omega \in \Omega_{[F;k]} \mid \omega = 0 \text{ or } D \leq (\omega)\}.\end{aligned}$$

We are now ready to state the Riemann-Roch theorem:

Theorem 24. (**Riemann-Roch Theorem**) Let $[F : k]$ be a function field with genus g and let $W \in \mathrm{Div}([F : k])$ be a canonical divisor (i.e. a canonical divisor of some Weil differential). Then, for all divisors $D \in \mathrm{Div}([F : k])$ we have the following equality:

$$\ell(D) - \ell(W - D) = \deg D + 1 - g.$$

Moreover, if $\deg D \geq 2g - 1$, then $\ell(W - D) = 0$ and thus in particular we get

$$\begin{aligned}\ell(D) &= \deg D + 1 - g \\ &\geq g.\end{aligned}$$

9 Elliptic curve cryptography

Elliptic curves forms a very special class of curves, which is intensively studied in both pure and applied areas because of the richness of the theories that can be developed onto it. An elliptic curve is nothing but a smooth curve of genus 1 in projective plane, which we have drawn below.

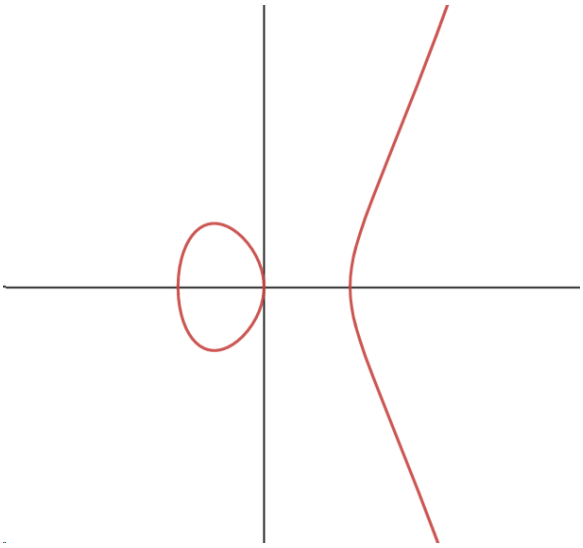


Figure 1: Elliptic curve $y^2 = x^3 - 2x$ in $\mathbb{A}^2(\mathbb{R})$.

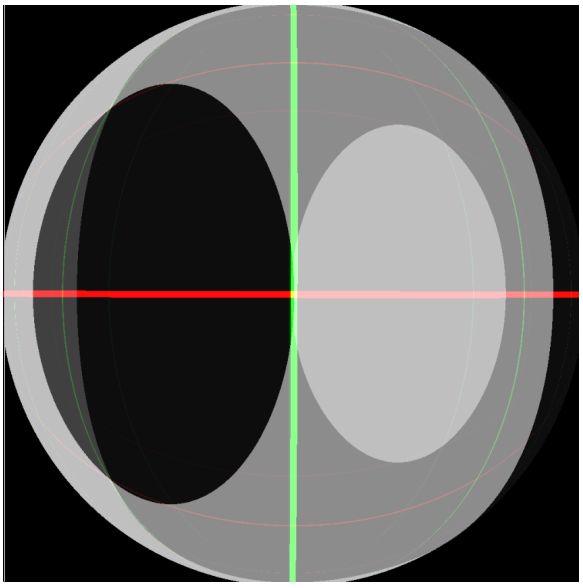


Figure 2: Interior of elliptic curve $y^2z = x^3 - 2xz^2$ in $\mathbb{P}^2(\mathbb{R})$ (shaded in dark black), the line on the right goes from north pole all the way to south. Also note the point $[0, 1, 0]$ is the north pole.

9.1 Group law of elliptic curves

Definition 9.1.1. (**Elliptic Curve over** k) Let k be a perfect field. A pair $(\mathcal{E}, O)$ is called an elliptic curve if $\mathcal{E}$ is a non-singular projective curve of genus 1 over k and O is a k-rational point of $\mathcal{E}$. The k-rational function field $k_{\mathcal{E}}$ is called an elliptic function field. Note that the k-rational point $O \in \mathcal{E}$ defines a closed point $\mathrm{Cl}\,(O) = \{O\}$ as O is k-rational. Now because k-closed points of a non-singular projective

curve are in bijection with places of the k-rational function field with degree of closed points and of places being same, therefore, associated to point O is a rational place of $[k_{\mathcal{E}} : k]$, which is also denoted by O.

Most of our focus will be towards the finite field case. With this in mind, we have the following example of an elliptic curve over a finite field. In particular, the following example shows one way of determining whether a projective curve is elliptic:

Example. *Elliptic curve over* $\mathbb{F}_2$. Consider the following projective curve $\mathcal{E}$ over $\mathbb{P}^2(\mathbb{F}_2)$:

$$y^2z + yz^2 - x^3 - xz^2 = 0.$$

One can check that each point of $\mathbb{P}^2(\mathbb{F}_2)$ of the form $[a, b, 1]$ where $a, b \in \mathbb{F}_2$ is a $\mathbb{F}_2$-rational point of $\mathcal{E}$. Of-course, $[0, 1, 0] \in \mathbb{P}^2(\mathbb{F}_2)$ is the only other $\mathbb{F}_2$-rational point of $\mathcal{E}$. Let us take $O = [0, 1, 0]$ to be the specified $\mathbb{F}_2$-rational point. We wish to show that $(\mathcal{E}, O)$ is an elliptic curve. For this we just need to show that $\mathcal{E}$ is a non-singular projective curve of genus 1. The fact that $\mathcal{E}$ is non-singular is easy to see via direct computation of Jacobian. The only thing remaining to see is that $\mathcal{E}$ indeed has genus 1. For this, we will use Riemann-Roch theorem. Firstly, consider the rational place corresponding to O, v_O, and we thus see that at point O, the rational function $x/1$ has a pole of order 2 because we first have to consider the homogeneous version of $x/1$, which is x/z, and thus:

$$\frac{x}{z} = \frac{y^2z + yz^2}{z(x^2 + z^2)} = \frac{y^2 + yz}{(x + z)^2}$$

and obviously, $(x + z)$ is zero at $O = [0, 1, 0]$. Also note that $y + yz$ is not zero at $O = [0, 1, 0]$. More compactly, we have $v_O(x) = 0 - 2$. Similarly, one can write the affine rational $y/1$ as y/z in projective space to obtain

$$\frac{y}{z} = \frac{y}{\frac{x^3+xz^2}{y^2+yz}} = \frac{y^2(y + z)}{x(x^2 + z^2)} = \frac{y^2(y + z)}{x(x + z)^2}.$$

Note that the final fraction is simple, that is, gcd of numerator and denominator is indeed 1. The above shows that the homogeneous rational polynomial y/z has a pole of order 3 and no zeros at $O = [0, 1, 0]$. That is, $v_O(y) = -3$.

We next have the main theorem in the theory of elliptic curves, which allows us to infer that k-rational points of an elliptic curve forms a group. For this, we first note that for any function field $[F : k]$, the set of all principal divisors form a subgroup of $\mathrm{Div}([F : k])$, so we denote this subgroup by $\mathrm{Princ}([F : k]) \leq \mathrm{Div}([F : k])$. Since $\mathrm{Div}([F : k])$ is an abelian group, therefore $\mathrm{Princ}([F : k])$ is normal and thus, we define the quotient group $\mathrm{Div}([F : k])/\mathrm{Princ}([F : k])$ to be the **divisor class group** of the function field $[F : k]$. It then follows by Corollary 3.4.3 of [NX09] that $\mathrm{Princ}([F : k])$ is a subgroup of $\mathrm{Div}([F : k])^0$ as well, the subgroup of all divisors of $[F : k]$ with degree 0. We then have the following result:

Theorem 25. Let $(\mathcal{E}, O)$ be an elliptic curve over field k. Denote by $\mathcal{E}(k)$ the set of all k-rational points of $\mathcal{E}$. Then the map

$$\begin{aligned} \chi : \mathcal{E}(k) &\longrightarrow \mathrm{Div}([k_{\mathcal{E}} : k])^0/\mathrm{Princ}([k_{\mathcal{E}} : k]) \\ P &\longmapsto \overline{P - O} \end{aligned}$$

where $\overline{P - O}$ denotes the canonical image under the projection $\mathrm{Div}([k_{\mathcal{E}} : k])^0 \to \mathrm{Div}([k_{\mathcal{E}} : k])^0/\mathrm{Princ}([k_{\mathcal{E}} : k])$, establishes a bijection between k-rational points of $\mathcal{E}$ and the group $\mathrm{Div}([k_{\mathcal{E}} : k])^0/\mathrm{Princ}([k_{\mathcal{E}} : k])$. Therefore, the k-rational points of an elliptic curve forms a group where the group law is inherited from the isomorphism χ.

Proof. This is Theorem 3.7.3 of [NX09]. ■

An affine plane curve over k defined by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is called a Weierstrass equation. We now see that every elliptic curve is isomorphic to homogenized version of Weierstrass equation:

Proposition 9.1.2. Let $(\mathcal{E}, O)$ be an elliptic curve over k. Then there exists an isomorphism φ of $\mathcal{E}/k$ to a homogenized Weierstrass curve $\mathcal{Y}/k$

$$\mathcal{Y} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $\varphi(O) = [0, 1, 0]$, that is, the specified k-rational point of $\mathcal{E}$ is mapped under this isomorphism to $[0, 1, 0]$, the north pole (see Figure 2).

Proof. This is Theorem 3.7.7 of [NX09]. ■

The above was introduced in order to state the following slogan : "the group law of an elliptic curve can be computed by the knowledge of the knowledge of points itself". This is formalized in the Corollary 3.7.9 of [NX09], refer there for more details because we won't need that technicality in the discussion presented here. Let us now present how this is used in cryptosystems in the next section.

9.2 Review of group based cryptography

Consider a sender A who wants to send a message m to a receiver B through a channel which is insecure, like internet. Also suppose that there is an eavesdropper E who has access to the channel (because it is insecure) who also wishes to know what m is while A and B doesn't want E to know what m is. Clearly, A cannot send m directly through the channel as E will know it. Hence, A and B has to agree on a *scheme* of encoding and decoding messages beforehand so to send the the message m securely through this channel. Thus arises the need for cryptography, the techniques of encoding and decoding messages so that the sender can reliably send the encoded message while being faithful that 1) it will infeasible for any eavesdropper to decode the message and 2) it can be decoded fairly easily by the intended receiver by a previously agreed scheme.

Let us now roughly spell out one instance of cryptosystems when the message to be conveyed is an element of a group. These systems are called group based cryptosystems and the following is a sketch of what is called the **ElGamal cryptosystem**. As usual, let A be the sender, B be the receiver and E be the eavesdropper. Let G be a group and $g \in G$ be a specified element such that $\operatorname{ord}(g)$, and hence $\operatorname{ord}(G)$, is large. Both the group G and element g is public knowledge. The message m which A wants to send to B is an element of the group G. In order to securely send m to B, A and B agree on the following scheme beforehand. B will select a random integer h which will be his private key (the data that only he is aware about, not even A) and he will send $b = g^h$ as the public key (everyone can know it). A, now having received b from B, also chooses a random integer k which will be it's private key and constructs the public key (c_1, c_2), where $c_1 = g^k$ and $c_2 = mb^k$. Now having received (c_1, c_2) from A insecurely, B can decode the actual message m via the following procedure: it computes $c_2c_1^{-h}$, which is $c_2c_1^{-h} = mb^kg^{-hk} = mg^{hk}g^{-hk} = m$. Thus B securely decodes message m from A.

Note that the eavesdropper E only was able to note b and (c_1, c_2) and thus it cannot decode m faithfully via just the knowledge of these two unless E can, in reasonable amount of time, solve the discrete logarithm problem for G, which asks the following: let $G = \langle g \rangle$ be a cyclic group generated by g and let $x \in G$. Find

the unique integer $0 \leq k \leq \text{ord}\,(G)$ such that $x = g^k$. It turns out that this problem depends on the group G and for many known groups, like multiplicative group of large finite fields, it is known to be infeasible in reasonable amount of time. Thus a necessary condition for ElGamal cryptosystem presented above is that the discrete log problem for group $\langle g \rangle \leq G$ must be infeasible.

9.3 ElGamal elliptic curve cryptosystem

In the previous section we saw how one can use large finite groups to establish a cryptosystem. In our study in the Part II, we were concerned with developing algebraic geometry from it's roots. Around the latter part, we briefly saw elliptic curves and realized that the set of k-rational points of an elliptic curve forms an abelian group, and it is a feature specific of elliptic curves (Theorem 25). We then saw that one can actually explicitly write the equation of an elliptic curve via Weierstrass equation and that the group law of $\mathcal{E}(k)$ can be understood completely in terms of it's affine coordinates (Proposition 9.1.2). We thus, for $k = \mathbb{F}_q$, obtain a finite abelian group $\mathcal{E}(k)$ which we would now like to use for cryptographic purposes. This is called the **ElGamal elliptic curve cryptosystem**.

We will use A, B and E as in the previous section and A wants to send a message M to B with E being an eavesdropper. Let $(\mathcal{E}, O)/\mathbb{F}_q$ be an elliptic curve over a finite field and let P be a specified $\mathbb{F}_q$-rational point of $\mathcal{E}$, both of which is public knowledge. For this discussion we will assume that messages are somehow encoded in the group $\mathcal{E}(\mathbb{F}_q)$, an assumption which we will question soon. Now, we begin with B. First, B cooks up a random integer h as its private key and publishes $Q = [h]P := P \oplus P \oplus \cdots \oplus P$ h times, as its public key. Then, having just received Q from B, A also cooks up a random integer k as it's private key and publishes (T_1, T_2) to the public where $T_1 = [k]P$ and $T_2 = M \oplus [k]Q$. Now, B receives (T_1, T_2) and it can decode message M using the following procedure:

$$T_2 \oplus [-h]T_1 = T_2 \oplus [-hk]P = M \oplus [k]Q \oplus [-hk]P = M \oplus [kh]P \oplus [-hk]P = M.$$

In order to make the finite group $\mathcal{E}(\mathbb{F}_q)$ large, it is enough to enlarge q via the famous Hasse-Weil bound which lower bounds the size of this group by $q + 1 - 2\sqrt{q}$. So in order to be infeasible to decrypt, we need to consider elliptic curves over large finite fields. Now, we still have to be sure somehow that the discrete log problem for $\langle P \rangle \leq \mathcal{E}(\mathbb{F}_q)$ is infeasible. It turns out that by a theorem of Pohlig-Hellman, the discrete log problem for $\langle P \rangle$ is infeasible if there is a large prime factor of $\text{ord}\,(P)$, otherwise it can be solved easily. So we want a large prime number to divide $\text{ord}\,(P)$, and thus $\text{ord}\,(\mathcal{E}(\mathbb{F}_q))$.

There is still an unanswered question in our discussion, that is, how can we embed a given message to be an $\mathbb{F}_q$-rational point of $\mathcal{E}/\mathbb{F}_q$? It is not a straightforward question and in general, we may not even know what are all the $\mathbb{F}_q$-rational points of an elliptic curve. Thus, there are various other cryptosystems having the same idea as ElGamal but assumes that message is not an $\mathbb{F}_q$-rational point but something else. One such example is that of Menezes & Vanstone's. As usual, let $\mathcal{E}/\mathbb{F}_q$ and an $\mathbb{F}_q$-rational point P of $\mathcal{E}$ be public knowledge. The message that A wants to send to B is now not an element of $\mathcal{E}(\mathbb{F}_q)$, but an element $M = (x_1, x_2) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, the product of multiplicative groups of $\mathbb{F}_q$. Then, as usual, B cooks up an integer h as its private key and publishes $Q = [h]P$ to the public. A receives Q and cooks up a random integer k as it's private key and publishes a triple (T, y_1, y_2) where $T = [k]P$, $y_1 = c_1 x_1$ and $y_2 = c_2 x_2$ to the public where $(c_1, c_2) = [k]Q$. Then B decodes (x_1, x_2) via the following procedure: B first finds (c_1, c_2) as follows

$$(c_1, c_2) = [k]Q = [kh]P = [hk]P = [h][k]P = [h]T$$

and then B finds $M = (x_1, x_2)$ as follows

$$(x_1, x_2) = (y_1 c_1^{-1}, y_2 c_2^{-1}).$$

References

[BJ01] F. Borceux, G. Janelidze, Galois Theories, Camb. Stud. Adv. Math. 72, Cambridge: Cambridge University Press (2001).

[Mac78] S. MacLane, Categories for the Working Mathematician, New York: Springer-Verlag, (1978).

[MM92] S. MacLane, I. Moerdijk, Sheaves in Geometry & Logic, A First Introduction to Topos Theory, Springer, New York, NY, (1992).

[DF03] D.S. Dummit, R.M. Foote, Abstract Algebra, John Wiley & Sons, 2003.

[Jan91] G. Janelidze, Pure Galois theory in categories, Journal of Algebra, Volume 132, Issue 2, 1 August 1990, Pages 270-286.

[Jan89] G. Janelidze, The fundamental theorem of Galois theory, Math. USSR Sbornik 64 (2), 1989, 359-374.

[Yan14] N. S. Yanofsky, Galois Theory of Algorithms, arXiv:1011.0014.

[Bor94] F. Borceux, Handbook of Categorical Algebra I, Cambridge University Press, 1994.

[Joh02] P. Johnstone, Sketches of an Elephant – A Topos Theory Compendium, Volume 2, Oxford University Press, 2002.

[NX09] H. Niederreiter, C. Xing, Algebraic Geometry in Coding Theory and Cryptography, Princeton University Press, 2009.