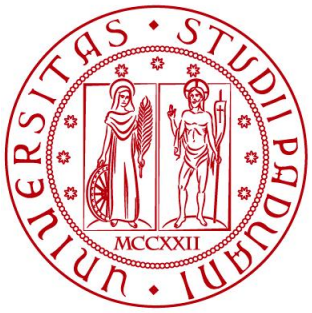


UNIVERSITÀ
DEGLI STUDI
DI PADOVA

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

An overview over the Infinite Galois Theory and Absolute Galois Groups

Relatore:
Prof. Riccardo Colpi

Laureando: **Giovanni Zanin**
Matricola: **2000429**

ANNO ACCADEMICO 2022/2023

22 settembre 2023

Contents

Introduction

Given its importance and notoriety, the Galois Theory is probably that subject that every mathematician has eventually crossed paths with. Its origins lie within the problem of finding a criterion for when with a polynomial equation of the form:

$$f(x) = 0$$

it is possible to obtain its roots only using radicals and standard arithmetic operations, but the results that were obtained thanks to it have gone way further than just arithmetic. It was between 1830 and 1832 that a young *Évariste Galois* sent his memoir to the Paris Academy of Science about his work regarding solvability by radicals, but got rejected due to the lack of formality. Luckily, the ideas in such papers were innovative and did not go unseen. His trick was to focus on a correspondence between two algebraic structures: groups and fields. Galois' major result, the "Fundamental Theorem of Galois Theory", asserts that when given a field F and a field extension satisfying some constraints Ω/F, called *Galois extension* there exists a bijection between intermediate fields $F \subset L \subset \Omega$ and subgroups of the *Galois group*, namely the groups $\mathrm{Gal}(\Omega/F) = \{\sigma \in \mathrm{Aut}(\Omega) | \sigma_{|F} = id_F\}$. A more formal characterization of all the *Galois extensions* was given some time later by *Emil Artin*, who gave some equivalent definitions. One important aspect of the *Galois extension* was that they were finite by definition, and as usually happens in mathematics, it is natural to think about what the outcome might be if this particular hypothesis is removed. For Galois Theory, this happened when the limitation of finite extensions was removed. The reason was that there were some quite easy algebraic field extensions that were normal and separable, but not finite. Unfortunately, as *Richard Dedekind* showed at the beginning of the 20th century, the Fundamental Theorem could not hold if given an infinite extension, and thus it required some more work that we will present in the following chapters:

- *Chapter 1* gives some basics of group theory, specifically properties of topological groups and inverse limits.
- *Chapter 2* is the core of this thesis and it focuses for real on the problem of Infinite Galois extensions. We will explicitly build a topology for an arbitrary Galois group and then prove the Fundamental Theorem of Galois Theory.

As stated earlier, there were already some known infinite separable and normal extensions, and particularly some were related to the *separable closure* of a field, and for this, we have:

- *Chapter 3*, that shows two particular cases of such infinite Galois extensions, focusing on the computation of the corresponding Galois group, called the *Absolute Galois Group*. The first example is related to finite fields, while the second to the more complex and sophisticated set of p-adic numbers.

Finite fields, sometimes also called *Galois fields*, have an especially easy extension structure and their Galois group are some of the easiest. Moreover, obtaining the absolute Galois group of a finite field is quite easy since it only relies on profinite groups, making finite fields a perfect example for the study of an infinite extension. The set of p-adic numbers, $\mathbb{Q}_p$, on the contrary, requires a lot more preliminaries in order to achieve such result. For this reason, in Chapter 3, we will first introduce normed spaces and discrete valuation rings, which are needed to define $\mathbb{Q}_p$, to study p-adic extensions, their basic properties and relations with finite fields. Secondly, some useful tools of ramification theory will be provided and used to finally compute the absolute Galois group.

Finally, at the bottom of this paper, there will be two appendixes. The first one contains basic concepts and results of finite Galois Theory, hence, the original results from Galois, while the second one is focused more on some elementary topological aspects.

Remark. *Please note that in what follows, unless specified, "field extension" is meant as "algebraic field extension".*

Acknowledgment

Before showing my work I would like to spend a few words to thank everyone who followed and supported me throughout these last three years and during the writing of this thesis.

Innanzitutto ringrazio il mio relatore Colpi Riccardo per la sua inesauribile pazienza e disponibilità, per avermi sempre fornito ogni materiale utile, ma soprattutto per la gentilezza e la fiducia riposte in me sin dal principio di questo progetto.

Non posso non ringraziare i miei genitori, due instancabili macchine da guerra, che nonostante tutto mi hanno sempre supportato in ogni scelta e percorso intrapreso. Da sempre mi spronate a dare il meglio di me, mi spingete ad inseguire i miei sogni e di fare di ogni conoscenza acquisita un tesoro, imparando a prendere il meglio di ogni cosa. In questi tre anni tortuosi non avete mai smesso di regalarmi amore e affetto e nonostante ciò che studio sia incomprensibile o poco convincente, non avete mai smesso di ascoltarmi e ve ne sono grato. Da voi ho imparato molto e probabilmente non smetterò mai di imparare.

Ringrazio di cuore anche la Nonna Bianca, perché hai sempre contribuito ai miei pasti e al supporto morale durante il mio percorso (ben più lungo di tre anni).

Estendo i miei ringraziamenti anche a tutti i colleghi di corso che hanno trascorso e condiviso con me le difficoltà e i traguardi, e a tutti gli amici nuovi e vecchi che hanno ben condito questi tre anni di studio.

Un grazie speciale va a mia sorella Sofia che nonostante la distanza fisica e il divario di interessi è sempre rimasta al mio fianco, sempre pronta a fornirmi consigli e a fare di ogni attimo assieme un'avventura memorabile, giusto per ricordarmi che qualche volta è buona norma far riposare un po' la mente.

Infine, ringrazio dal profondo del cuore Francesco. La tua presenza è stata fondamentale per la buona riuscita di questa tesi e di questa esperienza universitaria. Mi hai supportato, sopportato e costantemente stimolato ad immergermi sempre di più nel mondo della matematica. Sei stato il mio punto di riferimento e non posso che essere grato dell'amore e della felicità che mi hai dato fino ad oggi.

Chapter 1

Topological preliminaries

In this chapter, we will introduce a few topological structures and results required for the study of the Fundamental Theorem in Chapter 2, where we will show that all Galois groups associated with arbitrary Galois extensions do have a close connection to a specific topology. Please note that basic definitions, properties and results of topology can be found in Appendix B.

1.1 Topological groups

Definition 1.1.1. A set G together with a group structure and a topology is a *topological group* if the following maps are both continuous

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

$$\begin{aligned} {}^{-1} : G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned}$$

Following this request, we can show that if G is a topological group then the map:

$$\begin{aligned} a_L : G &\longrightarrow G \\ g &\longmapsto ag \end{aligned} \quad , a \in G$$

is a homeomorphism. It is firstly a continuous map because it is the composition of the injection of G in $G \times G$ and the multiplication map $\cdot$. Moreover, the map $(a^{-1})_L$ is inverse with a_L and continuous by definition.
Consequentially, if $H \subset G$ is a subgroup of G, the coset aH of H is open or closed according to H being open or closed.

Lemma 1.1.2. *Let G be a topological group and H a subgroup of G.*

1. *If H is open then is also closed;*
2. *If H is closed and of finite index is then open. Particularly, if G is compact and H is closed, H is open if and only if it is of finite index.*

Proof. Let H be an open subgroup of G. Then $G = \bigcup_{a\in G} aH$ and consequentially we have that $H = G/\bigcup_{a\in G, a\neq 1_G} aH$, being aH open. Such arbitrary union is still an open set of G as well meaning H is the complementary of an open set. Hence, closed. Let now H be a closed subset of finite index of G. Therefore, there exists a finite number of elements $a_1, ..., a_n \in G$, such that $G = \bigcup_{i=1}^{n} a_i H$, being $a_i H$ closed by hypothesis, their finite union is still closed and so H is the complementary of a closed set. Hence, open. Now, let G be compact and H a closed subgroup. If H is of finite index then is open thanks to what we have just proved. Conversely, if H is open, then the family of open sets $\{aH : a \in G\}$ is a covering for G. Being G compact, there exist $a_1, ..., a_n \in G$ such that $G = \bigcup_{i=1}^{n} a_i H$. This implies that H is of finite index. □

Recalling that a *neighbourhood base* for a point x of a topological space X is a set of neighbourhoods $\mathcal{N}$ such that for every open subset U of X containing x, there exists $N \in \mathcal{N}$ for what $N \subset U$. We can consequentially give the following result:

Proposition 1.1.3. *Let G be a topological group, and let $\mathcal{N}$ be a neighbourhood base for the identity element e of G. Then:*

1. *for all $N_1, N_2 \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $e \in N' \subset N_1 \cap N_2$*
2. *for all $N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $e \in N'N' \subset N$*
3. *for all $N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $e \in N' \subset N^{-1}$*
4. *for all $N \in \mathcal{N}$ and for all $g \in G$, there exists an $N' \in \mathcal{N}$ such that $N' \subset gNg^{-1}$*
5. *for all $g \in G$, $\{gN | N \in \mathcal{N}\}$ is a neighbourhood base for g.*

Conversely, if G is a group and $\mathcal{N}$ is a non-empty set of subsets of G satisfying the first four properties, then there is a topology on G for which the last propriety holds.

Proof. If $\mathcal{N}$ is a neighbourhood base at e in a topological group G, then (2), (3), (4) are consequences of the continuity of the multiplication and inversion maps. Moreover, (1) is a consequence of the definitions and (5) of the fact that the map g_L is a homeomorphism for every $g \in G$.

Conversely, let $\mathcal{N}$ be a nonempty collection of subsets of a group G satisfying the conditions from (1) to (4). Note that (1) implies that e lies in all the N in $\mathcal{N}$. Define now $\mathcal{U}$ to be the collection of subsets U of G such that, for every $g \in U$ there exists an $N \in \mathcal{N}$ with $gN \subset U$. Clearly, the empty set and G itself are in $\mathcal{U}$, and unions of sets in $\mathcal{U}$ are still contained in $\mathcal{U}$. Let $U_1, U_2 \in \mathcal{U}$, and $g \in U_1 \cap U_2$; by definition there exists $N_1, N_2 \in \mathcal{N}$ with $gN_1, gN_2 \subset U$; in applying (1) we obtain an $N' \in \mathcal{N}$ such that

$gN' \subset U_1 \cap U_2$, which shows that $U_1 \cap U_2 \in \mathcal{U}$. It follows that the elements of $\mathcal{U}$ are open sets of a topology on G. In fact, it is the unique topology for which (5) holds.

We next use (2) and (4) to show that the multiplication map is continuous. Note that the sets $g_1N_1 \times g_2N_2$ form a neighbourhood base for (g_1, g_2) in $G \times G$. Therefore, given an open subset U in G and a pair (g_1, g_2) such that $g_1g_2 \in U$, we have to find $N_1, N_2 \in \mathcal{N}$ such that $g_1N_1g_2N_2 \subset U$. As U is open, there exists an $N \in \mathcal{N}$ such that $g_1g_2N \subset U$. Apply (2) to obtain an N' such that $N'N' \subset N$, then $g_1g_2N'N' \subset U$. But $g_1g_2N'N' = g_1(g_2N'g_2^{-1})g_2N'$ and it remains to apply (4) to obtain an $N_1 \in \mathcal{N}$ such that $N_1 \subset g_2N'g_2^{-1}$.

Finally, we use (3) and (4) to show that the inversion map is continuous. Given an open subset U of G and a $g \in G$ such that $g^{-1} \in U$, we have to find an $N \in \mathcal{N}$ such that $gN \subset U^{-1}$. By definition, there exists an $N \in \mathcal{N}$ such that $g^{-1}N \subset U$. Now, $N^{-1}g \subset U^{-1}$, and we use (3) to obtain an $N' \in \mathcal{N}$ such that $N'g \subset U^{-1}$, and (4) to obtain an $N'' \in \mathcal{N}$ such that $gN'' \subset g(g^{-1}N'g) \subset U^{-1}$. □

1.1.1 Totally separable and totally disconnected spaces

Definition 1.1.4. Let X be a topological space then

1. Given an element $x \in X$, its *connected component* is the biggest connected set $C_x \subset X$ that contains x;

2. Given an element $x \in X$ its *quasicomponent* is the intersection of all clopen sets of X containing x.

Definition 1.1.5.

1. A topological space X is said to be *totally separable* if for every two distinct points, there exists a clopen set that separates them;

2. A topological space X is said to be *totally disconnected* if the connected component of every point $x \in X$ is the set $\{x\}$ itself.

Proposition 1.1.6. *A topological space X is totally separable if and only if each of its quasicomponent is a singleton set.*

Proof. ($\Rightarrow$) By contradiction, suppose that there exist two distinct $x, y \in X$ such that they are in the same quasicomponent. By hypothesis, there exists a clopen set U such that separates x and y, but this implies that this specific set contains x, hence the quasicomponent containing x is contained in such set U. Hence, y cannot be part of the quasicomponent set that contains y by assumption.

($\Leftarrow$) Given two distinct points x,y, the quasicomponent of x is $\{x\}$, hence it separates x from y. □

There is lastly an important result that will not be proven that shows a crucial correlation between the connected components and the quasicomponents.

Lemma 1.1.7 (Shura-Bura's Lemma)**.** *[[1], p.171-172] Given a compact topological space X, quasicomponents and connected components coincide.*

1.2 Inverse Limits

Definition 1.2.1. Given a partially ordered set (I, $\leq$), it is said to be a *directed set*, and consequentially $\leq$ is said to be a *directed* partial order, if:

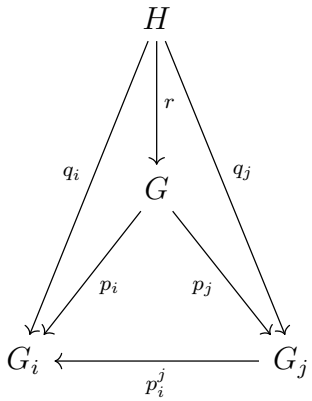
$$\forall i, j \in \text{I there exists } k \in \text{I such that } i, j \leq k$$

Definition 1.2.2. Let (I, $\leq$) be a directed set, and let $\mathcal{G}$ a family of groups

1. An *inverse system* in $\mathcal{G}$ indexed by (I, $\leq$), directed set, is a family $(G_j)_{j\in I}$ of groups of $\mathcal{G}$ together with a family $(p_i^j : G_j \to G_i)_{i\leq j}$ of homomorphisms such that $p_i^i = id_{G_i}$ and $p_i^j \circ p_j^k = p_i^k \ \forall i \leq j \leq k$

2. An object G of $\mathcal{G}$ together with a family $(p_j : G \to G_j)_{j\in I}$ of homomorphisms satisfying $p_i^j \circ p_j = p_i \ \forall i \leq j$, is an *inverse limit* of an inverse system, if G holds the following universal property:

   "For any other group H and family of homomorphisms $(q_j : H \to G_j)$ such that $p_i^j \circ q_j = q_i, i \leq j$, there exists a unique homomorphism $r : H \to G$ such that $p_j \circ r = q_j$ for $j \in I$"



Conventionally, the inverse limit of an inverse system of groups is written $\varprojlim(G_i, p_i^j)$ or just $\varprojlim(G_i)$. Now that we have the definition, we can consider a more specific case of inverse limit of a family of groups.
Let $(G_i, p_i^j : G_j \to G_i)$ be an inverse system of groups. Consider the set

$$G = \{(g_i)_i \in \prod_i G_i | p_i^j(g_j) = g_i \forall i \leq j\}$$

where the maps $p_i : G \to G_i$ are the usual projection maps. We can see that the property $p_i^j \circ p_j = p_i$ is equivalent to $p_i^j(g_j) = g_i$, which always holds in the set G by definition. Let now (H, q_i) be another family such that $p_i^j \circ q_j = q_i$ and let's consider the following map:

$$p\colon H \longrightarrow \prod_i G_i$$

$$h \longmapsto (q_i(h))_{i\in I}$$

We show that p is the map that follows the universal property of inverse limits.

1. We show that the image of the homomorphism is contained in G. Let $h \in H$ be a fixed element. Then

$$p(h) \in G \leftrightarrow p_i^j((p(h))_j) = (p(h)_i), \forall i \leq j \leftrightarrow p_i^j(q_j(h)) = q_i(h) \forall i \leq j$$

but by definition of the family (H, q_i) this is true;

2. We show that p respects the uniqueness property. Let $q : H \to \prod_i G_i$ be another homomorphism such that $p_i \circ q = q_i, \forall i \in I$. The image of q is in G because $q(h) \in G \leftrightarrow p_i^j((q(h))_j) = q(h)_i, \forall i \leq j$. By definition, $q(h)_i = (p_i \circ q)(h) = q_i(h)$ and $p_i^j((q(h))_j) = (p_i^j \circ p_j \circ p)(h) = (p_i^j \circ q_j)(h) = q_i(h)$. Let's now fix $i \in I$, then by assumption $p_i(q(h)) = q_i(h) = p_i(p(h)) \leftrightarrow p_i(p_i(h)(q_i(h)^{-1}) = 1_{G_i}$ and since the maps p_i are projections, this means that the entrance $(p_i(h)(q_i(h)^{-1})_i = 1_{G_i}$, but this is valid for all i meaning that $p \equiv q$.

Hence $(G, p_i) = \varprojlim(G_i, p_i^j)$. Note that the same result can be given if the groups are topological groups and $\prod_i G_i$ is endowed with the product topology. It is interesting to note that even if we have introduced the inverse limit based on group families, inverse limits are usually defined for categories by only replacing some terms in Definition 1.2.2. Besides that, this general definition will not be needed throughout the paper and the group-related one is enough.

After the introduction of inverse limits, we are in need of some properties of these structures, and from all of them the ones that we are interested in are proven in the following

Lemma 1.2.3. *The inverse limit S of an inverse system of non-empty compact Hausdorff spaces (groups) $\{S_i\}_{i \in I}$ given their (homo)morphisms π_i^j is a non-empty compact Hausdorff space (group).*

Proof. We first show that S is a closed subset of $\prod_{i \in I} S_i$. Suppose $s = (s_i)_i \in \prod_{i \in I} S_i$ does not belong to $\varprojlim(S_i) \Rightarrow \exists i, j \in I$ such that $i \leq j, \pi_{ji}(s_j) \neq s_j$. Let's now consider the open disjoint neighbourhoods U_i and $U_i^{'}$ of s_i and $\pi_{ji}(s_j)$ respectively, whom existence is certain thanks to the sets S_i being Hausdorff spaces. Then $U_i \times \pi_{ji}^{-1}(U_i^{'}) \times \prod_{k \neq i,j} S_k$ is an open neighbourhood of s in $\prod_{i \in I} S_i$ that does not intersect S. Since $\prod_{i \in I} S_i$ is compact thanks to Tychonoff's Theorem, S is a closed subset of a compact set, hence compact.
We now prove that S is nonempty. Let's define $R_{ij} = \{s \in \prod_{i \in I} S_i | \pi_{ki}(s_k) = s_j\}$ and consider $S = \bigcap_{k>j} R_{kj}$. The natural map: $pr_k \times pr_j : \prod_i S_i \to S_k \times S_j$ is continuous. The Hausdorff property of S_j implies that the set $T = \{(s_k, s_j) \in S_k \times S_j | \pi_{ki}(s_k) = s_j\}$ is closed in $S_k \times S_j$. Hence, $R_{kj} = (pr_k \times pr_j)^{-1}(T)$ is a closed subset of $\prod_{i \in I} S_i$. Since $\prod_{i \in I} S_i$ is compact, we only need to show that the intersection of finitely many of the R_{kj} is non-empty.
Indeed, let $j_1 \leq k_1, ..., j_n \leq k_n$ be n pairs in I. Choose $l \in I$ with $k_i \leq l, i = 1, ..., n$, and choose $s_l \in S_l$. Define $s_{j_i} = \pi_{l,j_i}(s_l)$ and s_{k_i}, for$i = 1, ..., n$. Let now s_r be an arbitrary element of S_r, for each $r \in I / \{j_1, ..., j_n, k_1, .., k_n\}$. Then $s = (s_i) \in \bigcap_{i=1}^n R_{k_i, j_i}$ □

1.3 Profinite Groups

In this subsection, we will introduce the notion of profinite groups, which are a particular type of inverse limits. The interest in profinite groups is large, but for this paper its introduction is mainly related to the fact that every Galois group will be proved to be a profinite group of some field extensions, giving us another view of both structures and properties of Galois groups.

Definition 1.3.1. Let G be a topological group. G is a *profinite group* if it is the inverse limit of an inverse system of finite groups, each one equipped with the discrete topology.

Proposition 1.3.2. *A topological group is profinite if and only if it is Hausdorff, compact and totally disconnected*

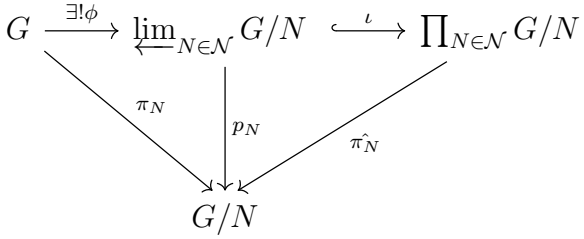
Proof. ($\Rightarrow$) Let $(G_i, p_i^j : G_j \to G_i)$ be an inverse system of finite groups and $G = \varprojlim G_i$. Thus,

$$G = \{(g_i)_i \in \prod_i G_i \colon p_i^j(g_j) = g_i \text{ all } i \leq j\}$$

If $(x_i) \notin G$, say $p_{i_0}^{j_0}(x_{j_0}) \neq (x_{i_0})$, then:

$$G \cap \{(g_j) | g_{j_0} = x_{j_0}, g_{i_0} = x_{i_0}\} = \emptyset$$

as the second set is an open neighbourhood of (x_i), this shows that G is closed in $\prod_i (G_i)$, which is compact by Tychonoff's Theorem (B.0.15), leading to the fact that G is also compact. Let now consider every map p_i, continuous by hypothesis for all i, and let U_i be its kernel. Such sets are all open and of finite index in G, hence closed, and $\bigcap_i U_i = \{e\}$. This implies that a subset of all the clopen sets containing the identity has its intersection consisting of only $\{e\}$ hence the quasicomponent of e is $\{e\}$. We have just proved that G is compact and thanks to the Shura-Bura's Lemma (1.1.7) the connected component of the identity is precisely $\{e\}$. Hence, for homogeneity, G is totally disconnected. Lastly, since G is the inverse limit of finite groups, from Lemma 1.2.3 and from the fact that all discrete topological groups are Hausdorff, G is Hausdorff.
($\Leftarrow$) Now, knowing that G is Hausdorff, totally disconnected and compact, we want to prove that G is isomorphic to the inverse limit of all quotients, G/N, where N represent an open normal subgroup. This family of sets is an inverse system made of nonempty Hausdorff compact sets, hence for Lemma 1.2.3 its inverse limit H is a Hausdorff nonempty compact set. We can see that the family $\{G, \pi_N | G \to G/N\}$ of natural projections is such that there exists a unique morphism ϕ from $G \to H$ thanks to the universal property of the inverse limit. We have to prove that this map is a bijection and continuous. To prove this statement we study the following commutative diagram where the symbol $\mathcal{N}$ indicates the set of all the normal subgroups of G:



1. injectivity; By looking at the diagram we can state that given an element $g \in G$ then

$$g \in \ker\phi \leftrightarrow \phi(g) = 1 \leftrightarrow \forall N \in \mathcal{N}, \hat{\pi_N}(\iota \circ \phi(g)) = 1$$
$$\leftrightarrow \forall N \in \mathcal{N}, p_N(\phi(g)) = 1 \leftrightarrow \forall N \in \mathcal{N}, \pi_N(g) = 1 \leftrightarrow g \in \bigcap_{N\in\mathcal{N}} N$$

but thanks to the hypothesis such intersection is the connected component of the identity element, meaning that g is the identity element. ϕ is consequentially injective;

2. continuity; From the fact that G is a topological group and G/N are endowed with the discrete topology, given a normal open subgroup N, the maps π_N and $\hat{\pi_N}$ are always continuous, thus p_N is continuous as well. Thanks to Lemma 1.2.3, we know that the inverse limit is Hausdorff and compact, and G/N are Hausdorff and compact as well thanks to the discrete topology, hence the map p_N is also closed (B.0.14) and every closed subset C in $\varprojlim_{N\in\mathcal{N}} G/N$, $p_N(C)$ is closed in G/N, too. Finally, thanks to the fact that π_N is continuous $\pi_N^{-1} \circ p_N(C)$ is closed in G. Thus, ϕ is continuous;

3. surjectivity; Let's denote with S a directed set that indices all open normal subgroups of G and let $(g_sN_s)_{s\in S}$ be an element of H. Then, by proposition 1.1.2 each N is a non-empty closed subset of G. Let's suppose that $\bigcap_{s\in S} g_sN_s =$. Then because G is compact, there is some finite collection $s_1, ..., s_n \in S$ such that $\bigcap_{i=1}^n g_{s_i}N_{s_i} = \emptyset$. Since the sets N form an inverse system, there must be an element s of S, with $s \geq s_1, ...s_n$ and by definition of inverse limit, we have $g_sN_s \subset \bigcap_{i=1}^n g_{s_i}N_{s_i}$, but as shown before the set N_s is non-empty, yielding a contradiction.

Thanks to this we have shown that G is a profinite group. □

Remark. *This proof hides an interesting trick for generating profinite groups when given a generic group G. To be precise, when G was a topological group we associated the inverse limit of G/H where H was running over normal open subgroups, to prove that G was actually the inverse limit itself. Similarly, if we are given a group G then we can still compute the inverse limit of G/H, where H runs over all normal subgroups of G and the result is called the "profinite completion" of G, written* $\hat{G}$.

Remark. *The previous observation and the result in the proposition lead us to the fact that every profinite group G is always isomorphic to the inverse limit of its quotient G/N, N being a normal open subgroup of G.*

It is remarkable that what we proved in Proposition 1.3.2, together with the observations, is precisely the topological key for the already mentioned correspondence between Galois groups and profinite groups. That is thanks to the fact that now we know how to associate profinite groups with generic groups and how strict their topological features are. Finally, right before exploring the correspondence in detail, we conclude this chapter with an example of a profinite group that will come back in hand further in the paper:

Example 1.3.3. Let (I, $\leq$) = ($\mathbb{N}$, $\preceq$), the set of natural numbers with the ordering defined by the division operator: $x \preceq y \leftrightarrow x$ divides y.
We then define the following inverse system:

$$\{\mathbb{Z}/n\mathbb{Z}, \phi_{mn}\}, \text{ where } \begin{array}{c} \phi_{mn}\colon \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \\ x + n\mathbb{Z} \longmapsto x + m\mathbb{Z} \end{array} \text{ for every } m \preceq n$$

and call $\hat{\mathbb{Z}}$ its inverse limit. Such set is the *profinite completion of* $\mathbb{Z}$ and in particular:

$$\hat{\mathbb{Z}} = \{(x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z} | m \preceq n \Longrightarrow x_n \equiv x_m \text{mod } m\}$$

We can also easily embed all the integers with the following map:

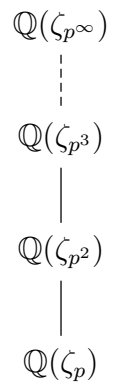
$$\begin{array}{c} i\colon \mathbb{Z} \longrightarrow \hat{\mathbb{Z}} \\ x \longmapsto (x + n\mathbb{Z})_{n\in\mathbb{N}} \end{array}$$

consequentially showing that $\mathbb{Z}$ forms a dense subset of $\hat{\mathbb{Z}}$, making this last one is topological closure, but being $\mathbb{Z}$ also a cyclic group generated by 1, we can more specifically say that it is the topological closure of the generator itself.

Chapter 2

Fundamental Theorem for Galois Extensions

We have already stated in the introduction of this paper that the theorem proved by Galois fails when the finite hypothesis is taken away, but we have yet to give a clear example of when this happens. Let p be a prime number and $\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n\leq 1} \mathbb{Q}(\zeta_{p^n})$ be the extension of rational numbers over the powers of the primitive p^n-th root of the complex unit. This gives us the following lattice:



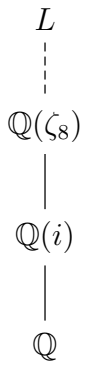
According to the finite case, $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ by the morphism σ such that $\sigma(\zeta_{p^n}) = (\zeta_{p^n})^{a_n}$ for some integer a_n mod p^n, where $GCD(a_n, p) = 1$.
Given an element $\sigma \in \mathbb{Q}(\zeta_{p^\infty})$, we get a list of numbers $a_n \mathrm{mod}\ p^n$ in $(\mathbb{Z}/p^n\mathbb{Z})\times$, which are not independent of each other. There is in fact a compatibility condition between them since for every n we have $(\zeta_{p^{n+1}})^p = \zeta_{p^n}$. Following from this we can assert that:

$$\sigma((\zeta_{p^{n+1}})^p) = \sigma(\zeta_{p^n}) \Rightarrow (\sigma(\zeta_{p^{n+1}}))^p = (\zeta_{p^n})^{a_n} \Rightarrow ((\zeta_{p^{n+1}})^{a_{n+1}})^p = (\zeta_{p^n})^{a_n} \Rightarrow (\zeta_{p^n})^{a_{n+1}} = (\zeta_{p^n})^{a_n}$$

so $a_{n+1} \equiv a_n \mathrm{mod}\ p^n$. The condition we found can occur in two cases only: when a_n is an integer or if $a_n = 1 + p + ... + p^{n-1}$.

Now that we have a specific construction, we study our counterexample considering

p=2 and denoting with L and $\mathbb{Q}$ the sets $\mathbb{Q}(\zeta_{p^\infty})$ and $\mathbb{Q}(\zeta_2)$, respectively.



For every odd number $a \in \mathbb{Z}$ let σ_a be the morphism in $\mathrm{Gal}(L/\mathbb{Q})$ such that elevate the p^n-th primitive root to the power of a. In this example we will consider when $a = 5, 13$ and we will call $H := \langle\sigma_5\rangle$ and $H' := \langle\sigma_{13}\rangle$. First of all, if $H = H'$ then the generator for σ_{13} would be one of the two generators $\sigma_5^{\pm 1}$ of H, which would mean that $13 \equiv 5^{\pm 1} \mathrm{mod}\ 2^n$ *for all* n but this would also mean that 13=5 or 13= 5^{-1} which is incorrect. Let's notice that this equivalence is not always wrong, for example, if $n = 2$ we have that $5, 13 \equiv 1\mathrm{mod}\ 4$. Also, since the extension $\mathbb{Q}(\zeta_4)$ is equal to $\mathbb{Q}(i)$ and 5,1/5 and 13 are different in $\mathbb{Q}$, we can say that the element i is fixed by both σ_5 and σ_{13}.

In order to understand why this situation really is a counterexample, we have prove the following lemma:

Lemma 2.0.1. *Let $a \in \mathbb{Z}$ be such that $a \equiv 1\mathrm{mod}\ 4$ and $a \not\equiv 1\mathrm{mod}\ 8$ then the subgroup generated by a in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ has index 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times, n \in \mathbb{N}$.*

Proof. Firstly we observe that the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is composed of only the element of $\mathbb{Z}/2^n\mathbb{Z}$ such that are coprime with 2^n, hence all the odd numbers between 1 and $2^n - 1$ which are precisely 2^{n-1}. We now have to compute the multiplicative order of a. To do so, we need some results.

- By induction we prove that for every non-negative integer k, $a^{2^k} \equiv 1 \mod 2^{k+2}$. It is true for $k = 0$ by hypothesis. Let's now assert that $a^{2^k} \equiv 1 \mod 2^{k+2}$ holds, we prove that the statement is correct also for $k + 1$. $a^{2^{k+1}} = (a^{2^k})^2 \equiv 1 \mod 2^{k+3}$ if and only if a^{2^k} is equivalent to $1, -1, 2^{k+2} + 1$ or $2^{k+2} - 1 \mod 2^{k+3}$. By hypothesis, we can assert that $a^{2^k} \equiv 1 \mod 2^{k+3}$ or $a^{2^k} \equiv 1 + 2^{k+2} \mod 2^{k+3}$.

- We now prove by induction that for every non-negative integer k, $a^{2^k} \not\equiv 1 \mod 2^{k+3}$. It is true for $k = 0$ by hypothesis. Let's now assert that $a^{2^k} \not\equiv 1 \mod 2^{k+3}$ holds, we prove that the statement is correct also for $k + 1$. $(a^{2^k})^2 = a^{2^{k+1}} \not\equiv 1 \mod 2^{k+4}$ holds if and only if $a^{2^k} \not\equiv 1, -1, 1 + 2^{k+3}$ or $-1 + 2^{k+3} \mod 2^{k+4}$. Consequentially, the property holds if and only if $a^{2^k} \not\equiv 1, -1 \mod 2^{k+3}$, which is true by hypothesis.

Now, with this in mind, let's consider $k = n - 2, n \geq 3$. Then $a^{2^{n-2}} \equiv 1 \mod 2^n$ and we prove that $2^{n-2} = |a|$. Let now $1 \leq l < n - 2$ be a positive integer such that $a^{2^{n-2-l}} \equiv 1 \mod 2^n$ and observe that $n - l + 1 < n$, since $1 \leq l$. Now, we observe that $a^{2^{n-2-l}} \equiv 1$

mod $2^n \Rightarrow a^{2^{n-2-l}} \equiv 1 \mod 2^{n-1+l}$, and if we define the following integer $k := n - l - 2$ we have that $a^{2^k} \equiv 1 \mod 2^{k+3}$, which has been proven wrong. Finally, we have that $\langle a \mod 2^n \rangle$ has index $2^{n-1}/2^{n-2} = 2$. □

Furthermore, we can notice that the relation between 5 and 13 actually holds for every positive integer n bigger than 2, and so $\langle 5 \mathrm{mod}\ 2^n \rangle = \langle 13 \mathrm{mod}\ 2^n \rangle$ and since neither of them is equivalent to 1mod 8, they both have index 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. This index means that despite the integer n the fixed field will always be $\mathbb{Q}(i)$ because it has degree 2 over $\mathbb{Q}$. But this also means that $L_H = \mathbb{Q}(i) = L'_H$. So we have found a situation where even if two subgroups are different, H, H', the Galois correspondence still gives us the same exact intermediate field.

This example was described by R. Dedekind in 1901 and it clearly proves that if given an infinite algebraic extension, which is still separable and normal, it does not follow the Fundamental Theorem of Galois theory, which is why we have been calling it "Fundamental Theorem of Finite Galois Theory" since then. The Galois correspondence, so powerful in the finite case, needs to be fixed for the infinite case, and the idea to solve this issue was given by W. Krull.

2.1 The Krull Topology

Recall that in order to define a Galois extension three specific characteristics are required: given Ω/F an algebraic field extension, it is said to be *Galois* if finite, normal and separable (Definition A.2.3), implying that for every irreducible polynomial $f \in F[X]$ that has a root in Ω, it also has deg$f$ distinct roots in Ω. What we want to do is to get rid of the finiteness hypothesis, while still preserving all the results already proven for the finite case. To do so, from now on we will consider the property of being a "Galois extension" as follows:

Definition 2.1.1. Let Ω/F be an algebraic extension, then Ω is said to be *Galois* over F if Ω/F is a normal and separable field extension of F.

Proposition 2.1.2. *If Ω is Galois over F, then it is Galois over every intermediate field M.*

Proof. Let *f(x)* be an irreducible polynomial in *M[X]* having a root α in Ω. The minimal polynomial *g(x)* of α over F splits into distinct factors of degree one in $\Omega[X]$. As f divides g (in *M[X]*), it also split into distinct factors of degree one in Ω*[X]*. □

Proposition 2.1.3. *Let Ω be a Galois extension over F and let E be a subfield of Ω containing F. Then every F-homomorphism between E and Ω can be extended to an F-isomorphism in Ω.*

Proof. The proof that an F-homomorphism between E and Ω extends to a homomorphism $\alpha : \Omega \to \Omega$ can be found in the [[6], p.90]. Let's now consider $a \in \Omega$, and f its minimal polynomial over F. Then Ω contains exactly deg*(f)* roots of f, and so therefore does $\alpha(\Omega) \subset \Omega$. Hence $a \in \alpha(\Omega)$, which shows that α is surjective. □

Corollary 2.1.4. *Let $F \subset E \subset \Omega$ be as in Proposition 2.1.3. If E is stable under* $\mathrm{Aut}(\Omega/F)$ *then E is Galois over F.*

Proof. Let *f(x)* be an irreducible polynomial in *F[X]* having a root $a \in E$. Because Ω is Galois over F, f has $n := deg(f)$ distinct root $a_1, ..., a_n \in \Omega$. There is an F-isomorphism $F(a) \to F(a_i) \subset \Omega$ sending a to a_i, which extends to an F-isomorphism $\Omega \to \Omega$. As E is stable under $\mathrm{Aut}(\Omega/F)$, this shows that $a_i \in E \ \forall i$. □

Let Ω be a Galois extension of F, and let $G := \mathrm{Aut}(\Omega/F)$. We consider, for every finite subset S of Ω the following set:

$$G(S) = \{\sigma \in G | \sigma s = \text{ s for all s} \in S\}$$

and with the family of sets $\{G(S)\}_{S \subset \Omega \text{ finite}}$ we want to induce a topology over the group $\mathrm{Aut}(\Omega/F)$. For this, we prove the following proposition:

Proposition 2.1.5. *There is a unique structure of a topological group on G for which the sets G(S) form an open neighbourhood base of the identity. For this topology, the sets G(S) with S being stable under G action, form a neighbourhood base of the identity consisting of open normal subgroups.*

Proof. We show that the first four conditions of Proposition 1.1.3 are satisfied by the *G(S)* sets collection.
(1) is satisfied because $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$;
(2) and (3) are satisfied because each set *G(S)* is a group;
Let now S be a finite subset of Ω. Then *F(S)* is a finite extension of F, and so there are only finitely many F-homomorphisms between *F(S)* $\to \Omega$ (A.3.2). Since $\sigma S = \tau S$ if $\sigma_{|F(S)} = \tau_{|F(S)}$, this shows that $\overline{S} = \bigcup_{\sigma \in G} \sigma S$ is finite. Now, $\sigma \overline{S} = \overline{S}$ for all $\sigma \in G$, and it follows that $G(\overline{S})$ is normal in G. Therefore, $\sigma G(\overline{S}) \sigma^{-1} \subset G(S)$, which proves (4). This also proves the second statement. □

Therefore, if S is a finite set stable under G, then *F(S)* is a finite extension of F stable under G and hence Galois over F. The following set is consequentially a neighbourhood base of the identity consisting of open normal subgroups:

$$\{\mathrm{Gal}(\Omega/E) |\ E \text{ finite and Galois over } F\}$$

This observation also leads us to the following proposition:

Proposition 2.1.6. *Let Ω be Galois over F. For every intermediate field E finite and Galois over F, the map:*

$$\begin{aligned} \phi_E : \mathrm{Gal}(\Omega/F) &\longrightarrow \mathrm{Gal}(E/F) \\ \sigma &\longmapsto \sigma_{|E} \end{aligned}$$

is a continuous surjection ($\mathrm{Gal}(E/F)$ *embedded with the discrete topology)*

Proof. Let $\sigma \in \mathrm{Gal}(E/F)$ and regard it as an F-homomorphism between E and Ω. Then σ can be extended as an F-automorphism in Ω thanks to the Proposition 2.1.3, which shows that the map ϕ_E is a surjection. For every finite set S of generators of E over F, $\mathrm{Gal}(\Omega/E) = G(S)$, which shows that the inverse image of $1_{\mathrm{Gal}(E/F)}$ is open in G. By homogeneity, the same is true for every element of $\mathrm{Gal}(E/F)$. □

The topology obtained on $\mathrm{Aut}(\Omega/F)$ by this proposition is called *Krull topology* and the group $\mathrm{Aut}(\Omega/F)$ endowed with this said topology is called *Galois group of* Ω/F, denoted with $\mathrm{Gal}(\Omega/F)$.

Remark. *When given a Galois group* $\mathrm{Gal}(\Omega/F)$ *endowed with the Krull Topology, where all the open sets are all related to intermediate finite Galois extension, it is easy to see that any intermediate subfield of* Ω *containing* F *is Galois if and only if it is the union of finite Galois extensions of* F*.*

Proposition 2.1.7. *The Galois group* G *of a Galois extension* Ω/F *is Hausdorff, compact and totally disconnected.*

Proof. We first show that G is Hausdorff. If $\sigma \neq \tau \Rightarrow \sigma^{-1}\tau \neq 1_G$, and so it moves some element of Ω, i.e. there exists an $a \in \Omega$ such that $\sigma(a) \neq \tau(a)$. For every S containing a, $\sigma G(S)$ and $\tau G(S)$ are disjoint subgroups because their elements act differently on a. Hence they are disjoint open subsets of G containing σ and τ respectively

We now show that G is compact. As we noted above, if S is a finite set in Ω stable under G, then $G(S)$ is a normal subgroup of G, and it has finite index because it is the kernel of the immersion of G inside $\mathrm{Sym}(S)$, which is specifically the group of all different permutation of the elements of S which has cardinality $|S|!$. Given an arbitrary element $\alpha \in \Omega$ we observe that it is first of all algebraic over F and secondly it is such that the set $\{\sigma(\alpha)\}_{\sigma \in G}$, called *orbit*, is composed only by the roots of its minimal polynomial, which come in finite number thanks to Ruffini's Theorem. This tells us that every finite set is contained in a stable finite set and the following map is consequentially injective:

$$G \to \prod_{S \text{ finite stable under } G} G/G(S)$$

Notice that if we endow $\prod_S G/G(S)$ with the product topology, the induced topology on G is that for which the $G(S)$ form an open neighbourhood base of the identity, i.e. the Krull topology. Now, according to Tychonoff's Theorem, $\prod_S G/G(S)$ is compact, and so it remains to show that G is closed in the product. For each $S_1 \subset S_2$, there are two continuous maps $\prod_S G/G(S) \to G/G(S_i)$, for $i = 1, 2$, namely, the natural projections. This is followed by the quotient map $G/G(S_1) \to G/G(S_2)$. Let $E(S_1, S_2)$ be the closed subset of $\prod_S G/G(S)$ on which the two maps agree. Then $\bigcap_{S_1 \subset S_2} E(S_1, S_2)$ is closed and equals the image of G. Finally, for each finite set S stable under G, $G(S)$ is a subgroup that is open and hence closed. Basically, it is a family of clopen sets in G. Since $\bigcap_{S \text{ finite stable under } G} G(S) = \{1_G\}$. Thanks to the already proven compactness and Lemma 1.1.7 this shows that the connected component of G containing 1_G is $\{1_G\}$ itself. By homogeneity, G is totally disconnected. □

Proposition 2.1.8. *Let G be a group of automorphisms of a field E, and let $F = E_G$ (definition at Theorem A.4.4). If G is compact and the stabilizer of each element of E is open in G, then E is a Galois extension of F with Galois group G*

Proof. Let $x_1, x_2, ..., x_n$ be a finite set of elements of E, and let H_i be the open subgroup of G fixing x_i. Because G is compact, the set $Gx_i : \{\sigma(x_i)\}_{\sigma \in G}$ of x_i is finite, and the subgroups of G fixing its elements are the conjugates of H. Let N be the intersection of all the subgroups of H_i. It is an open normal subgroup of x_i. Thus, G/N is a (finite) group of automorphisms of M with fixed field F. According to Artin's Theorem (A.4.4), M is a finite Galois extension of F with Galois group G/N. As E is a directed union of such fields M, it is a Galois extension of F. Thus, $\mathrm{Gal}(E/F)$ is defined and by assumption G maps itself continuously and injectively into it. Such image is also closed thanks to G compactness and it is dense because it maps onto all the group $\mathrm{Gal}(M/F)$. Thus, $G \to \mathrm{Gal}(E/F)$ is an isomorphism. □

Proposition 2.1.9. *For every Galois extension Ω/F, $\Omega_{\mathrm{Gal}(\Omega/F)} = F$.*

Proof. Every element of Ω/F lies in a finite Galois extension of F, and so this follows from the surjectivity proven in Proposition 2.1.6. □

Remark. *Following from this proposition and Proposition 1.3.2 we can assert that every Galois group of a Galois extension is indeed a profinite group. The vice versa also holds as every profinite group is the Galois group of some field extension:*

Proof. Let G be a profinite group and let S be the disjoint union of the sets G/H, given the open subgroup $H \subset G$. Then G acts faithfully on S, i.e. give $g \in G$ if $g(s) = s, \forall s \in S \Rightarrow g = 1_G$, and the stabilizer of each element of S is open in G. Let K be a field and $K(S)=:E$ be the field of fractions of $K[S]$, the polynomial ring over K in the elements of S. Then, G acts faithfully on E through its action on S and the stabilizer of each element in E is consequentially open in G. According to Proposition 2.1.8, E is Galois over $F := E_G$ with Galois group G. □

2.2 The Fundamental Theorem

Proposition 2.2.1. *Let Ω/F be a Galois extension and G its Galois group. Let's define for every subgroup H of G the following set $\Omega_H := \{\alpha \in \Omega | \sigma\alpha = \alpha, \forall \sigma \in H\}$, then:*

1. *If M is a subfield of Ω containing F, then Ω is Galois over M, the Galois group $\mathrm{Gal}(\Omega/M)$ is closed in G and $\Omega_{\mathrm{Gal}(\Omega/M)} = M$;*

2. *For every subgroup $H \subset G, \mathrm{Gal}(\Omega/\Omega_H)$ is the closure of H.*

Proof. 1. The first assertion was proved in 2.1.2. For each finite subset $S \subset M$, $G(S)$ is an open subgroup of G, hence closed. Also, $\mathrm{Gal}(\Omega/M) = \bigcap_{S \subset M} G(S)$ is closed as well. The final statement follows from 2.1.9.

2. Since $\mathrm{Gal}(\Omega/\Omega_H)$ is a closed set containing H, it certainly contains H's closure $\overline{H}$. Let's now consider $\sigma \in G/\overline{H}$ and we show that σ moves some element of Ω_H. Because σ is not in H's closure:

$$\sigma(\mathrm{Gal}(\Omega/E)) \cap H = \emptyset$$

for some finite Galois extension E of F in Ω (because the sets $\mathrm{Gal}(\Omega/E)$) form a neighbourhood of the identity). Let Φ denote the surjective map $\mathrm{Gal}(\Omega/E) \to \mathrm{Gal}(F/E)$. Then $\sigma_{|E} \notin \Phi(H)$ and so σ moves some element of $E_{\Phi(H)} \subset \Omega_H$. □

Now that all the preparations have been made we are finally ready to prove the milestone of the infinite Galois Theory:

Theorem 2.2.2. *(Fundamental Theorem of Galois Theory) Let Ω be a Galois extension of F with Galois group G. Then the maps:*

$$\Omega_H \longleftarrow H$$

$$M \longrightarrow \mathrm{Gal}(\Omega/M)$$

are inverse bijections between the set of closed subgroups of G and the set of intermediate fields between Ω and F:

$$\{H \subset G | H \text{ closed in } G\} \longleftrightarrow \{M | F \leq M \leq \Omega, M \text{ subfield}\}$$

Moreover,

1. *$H_2 \subset H_1 \iff \Omega_{H_1} \subset \Omega_{H_2}$ Meaning that the found correspondence is order reversing.*
2. *A closed subgroup H of G is open if and only if Ω_H has finite degree over F. In this case: $(G : H) = [\Omega_H : F]$*
3. *For every $\sigma \in G$, $\sigma H \sigma^{-1} \leftrightarrow \sigma M$, i.e.*

$$\Omega_{\sigma H \sigma^{-1}} = \sigma(\Omega_H);$$

$$\mathrm{Gal}(\Omega/\sigma M) = \sigma\,\mathrm{Gal}(\Omega/M)\sigma^{-1}$$

4. *A closed subgroup H of G is normal if only if Ω_H is Galois over F, in which case:*

$$\mathrm{Gal}(\Omega_H/F) \equiv G/H$$

Proof. For the first statement, we have to show that the two defined functions are indeed inverse maps. Let H be a closed subgroup of G. Then Ω is Galois over Ω_H and $\mathrm{Gal}(\Omega/\Omega_H) = H$ (see 2.2.1) Let M be an intermediate field, then $\mathrm{Gal}(\Omega/M)$ is a closed subgroup of G and $\Omega_{\mathrm{Gal}(\Omega/M)} = M$ (See 2.2.1)

1. We have the following obvious implications:

$$H_1 \supset H_2 \Rightarrow \Omega_{H_1} \subset \Omega_{H_2} \Rightarrow \mathrm{Gal}(\Omega/\Omega_{H_1}) \supset \mathrm{Gal}(\Omega/\Omega_{H_2})$$

As $\mathrm{Gal}(\Omega/\Omega_{H_i}) = H_i$, this proves the first statement.

2. Let H be an open subgroup of G. Since G is a topological compact group, H is also closed and must have finite index $(G : H)$. The map $\sigma \mapsto \sigma_{|\Omega_H}$ defines a bijection between G/H and $\mathrm{Hom}_F(\Omega_H, \Omega)$ from which the statement follows (2.1.3).

3. For $\tau \in G$ and $\alpha \in \Omega, \tau\alpha = \alpha \leftrightarrow \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha$.
Therefore, $\mathrm{Gal}(\Omega/\sigma M) = \sigma \,\mathrm{Gal}(\Omega/\sigma M)\sigma^{-1}$, and so $\sigma H\sigma^{-1} \leftrightarrow \sigma M$.

4. Let $H \leftrightarrow M$. It follows from the previous point that H is normal if and only if M is stable under the action of G. But M is stable under the action of G if and only if it is a union of finite extension of F all of them stable under G. We have already observed that an extension is Galois if and only if it is a union of finite Galois extensions (remarked in section 2.1). Hence, H is normal if and only if M is Galois over F.

□

2.3 Galois groups as profinite groups

We have already proven that Galois Groups and profinite groups are two sides of the same coin: it is always possible to associate a Galois extension with a given profinite group and conversely, a Galois group is always a profinite group thanks to its topological properties. We could assert that in order to build a Galois Group of an infinite extension we could just use what we have proven in the Proposition 1.3.2. Right after the proof we observed that when given a group G it is possible to compute the inverse limit of the quotient classes G/N, running over the normal subgroups, and when G was in fact a topological group, the result was that such inverse limit was isomorphic to G itself. Besides how interesting and curious this strategy is, it is not the most efficient when trying to compute the Galois group for an infinite extension.

Galois groups are in fact a little special and for them there exists a more practical inverse limit. What we are going to prove is that $\mathrm{Gal}(\Omega/F) \simeq \varprojlim_{E/F \text{ finite Galois}} \mathrm{Gal}(E/F)$

Let Ω/F be a Galois extension of a field F. The composite of two finite Galois extensions in Ω is again a Galois extension (follows from Proposition A.4.6), and so if sorted by inclusion, all the intermediate finite Galois extensions in Ω/F form a directed set I. More specifically given two fields $F \leq E, E' \leq \Omega$ we say that $E \prec E' \leftrightarrow E \subset E'$ and also we can consider the restriction morphism

$$p_E^{E'} : \mathrm{Gal}(E'/F) \to \mathrm{Gal}(E/F)$$

We have consequentially obtained an inverse system $(\mathrm{Gal}(E/F), p_E^{E'})$. Alongside, we also have the couple $(\mathrm{Gal}(\Omega/F), p_E)$ where p_E represent the family of restriction homomorphisms $p_E : \mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F)$. This way, thanks to the universal property of inverse

limits we can define a homomorphism:.

$$\Phi : \mathrm{Gal}(\Omega/F) \longrightarrow \varprojlim_{E/F \text{ finite Galois}} \mathrm{Gal}(E/F)$$

$$\sigma \longmapsto (\sigma_{|\,\mathrm{Gal}(E/F)})_{\{E|E/F \text{ finite Galois}\}}$$

This specific map is also an isomorphism of topological groups.

- Let $\sigma \in \ker(\Phi)$, then $\sigma_{|\,\mathrm{Gal}(E/F)} = id_E$ for every finite Galois extension of F. Since $\Omega = \bigcup E$, $\sigma \equiv id_\Omega$. Φ is injective;

- Let now $(\sigma_E) \in \varprojlim \mathrm{Gal}(E/F)$, with$\sigma_E \in \mathrm{Gal}(E/F)$. Then we define $\sigma : \Omega \to \Omega$ such that $\sigma_{|E} \equiv \sigma_E$. σ is well-defined. Let E,E' be finite Galois extensions, then $E \cap E'$ is also a finite Galois extension.

  $$p^E_{E\cap E'}(\sigma_E) = \sigma_{E\cap E'}$$

  $$p^E_{E\cap E'}(\sigma_{E'}) = \sigma_{E\cap E'}$$

  thus σ_E and $\sigma_{E'}$ agree on $E \cap E'$. By construction, $\sigma_{|E} = \sigma_E$. Φ is surjective;

- Since we are working with topological groups we prove that Φ is also continuous. Let's consider the directed set I obtained from ordering all the finite Galois sub-extension of Ω/F and then the following topology for $\prod_{i\in I} \mathrm{Gal}(L_i/F)$:

  $$(g_i) \circ \Big(\prod_{i\neq i_1,\ldots,i_n} \mathrm{Gal}(E_i/F) \times \prod_{j=1}^{n} (id_{L_{i_j}})\Big)$$

  con $(g_i) \in \prod_{i\in I} \mathrm{Gal}(E_i/F)$. Let's define the following labels:

  - $H := \varprojlim \mathrm{Gal}(E/F)$
  - $K := \prod_{i\neq i_1,\ldots,i_n} \mathrm{Gal}(E_i/F) \times \prod_{j=1}^{n} (id_{L_{i_j}})$
  - $x := (g_i)$

  By definition, $(xK) \cap H \neq \emptyset$. Thus, there exist $y \in H, k \in K$ such that $y = xk$. Meaning that $yK = xK \Rightarrow (yK) \cap H = y(K \cap H)$. We have to prove that $\Phi^{-1}(y(K \cap H)) = \Phi^{-1}(y)\Phi^{-1}(K \cap H)$ is open in $\mathrm{Gal}(\Omega/F)$ for every $y \in H$. This is true because $\Phi^{-1}(K\cap H) = \mathrm{Gal}(\Omega/L_{i_1})\cap\ldots\cap\mathrm{Gal}(\Omega/L_{i_n})$ which is open in $\mathrm{Gal}(\Omega/F)$.

- Lastly, we prove that Φ is open. We show specifically that: $\Phi(\mathrm{Gal}(\Omega/L_s)) = \{(\sigma_{L_i}) \in \varprojlim \mathrm{Gal}(L_i/F) | \sigma_{L_s} = id_{L_s}\} =: T$

  It is clear that for every $\sigma \in \mathrm{Gal}(\Omega/L_s) \Rightarrow \Phi(\sigma) \in T$. Let's now consider $(\sigma_{L_i}) \in T$ and $\sigma = \Phi^{-1}((\sigma_{L_i}))$ such that $\sigma \in \mathrm{Gal}(\Omega/L_s)$ since $\sigma_{|L_s} = \sigma_{L_s} = id_{L_s}$. T is open in $\varprojlim \mathrm{Gal}(L_i/F)$ since $T = \varprojlim \mathrm{Gal}(L_i/F \cap (\prod_{i\neq s} \mathrm{Gal}(L_i/F) \times id_{L_s})$. Thus, $\Phi(\mathrm{Gal}(\Omega/L_i))$ is open for every $i \in I$. Thanks to the fact that Φ is a homomorphism we can assert that Φ is such that $\Phi(a\,\mathrm{Gal}(\Omega/L_i)) = \Phi(a)\Phi(\mathrm{Gal}(\Omega/L_i))$ are all open.

Chapter 3

The Absolute Galois Group

In this final chapter, we will examine a classic example of an infinite Galois extension of two specific fundamental fields: the first one is the well-known family of finite fields, while the second one is the intricate p-adic numbers field. From the very beginning, these two fields might look unrelated, but this will likely change. What we plan to do in this chapter is to fully compute the Galois group for a specific kind of infinite extension.

Definition 3.0.1. Let F be a field, then F is said to be *algebraically closed* if every polynomial $f \in F[x]$ splits in F.

Definition 3.0.2. Let Ω/F be a field extension, then it is called an *algebraic closure* of F if:

1. Ω/F is algebraic
2. Ω is algebraically closed

The property of being algebraically closed might sometimes be too strong, so we want to work with something weaker:

Definition 3.0.3. Given a field Ω, it is said to be *separably closed* if every separable polynomial in $\Omega[X]$ splits in Ω. Similarly to the algebraic closure, we say that when given a field extension Ω/F, Ω is a *separable closure* of F if it is algebraic, separable and separably closed.

When given a certain field, however, just like the algebraic closure, the separable closure is unique up to isomorphism. Hence, we give the following definition:

Definition 3.0.4. Let F be a field, and $\overline{F}$ an algebraic closure of F. We define the following set:

$$F_s = \{x \in \overline{F} | x \text{ is separable over } F\}$$

F_s is called the *separable closure* of F

Proposition 3.0.5. *Let E be a separable closure for a field F, then E is equal to F_s.*

Proof. By definition, E is a separable extension, hence every element in E must also be in F_s. On the other hand, given an element $\alpha \in F_s$ then its minimum polynomial $f_\alpha \in F[X]$ is separable, but since $F[X] \subset E[X]$, f_α is also separable in $E[X]$. Since E is separably closed then $\alpha \in E \Rightarrow F_s \subset E$. □

It is not hard to see that F_s/F is indeed a Galois extension. It's trivially separable and also normal. This is because when given an irreducible polynomial $f \in F[X]$ that has a root $\alpha \in F_s$, then α's minimum polynomial f_α is separable and $f_\alpha | f \Rightarrow f_\alpha = f$ meaning that every root of f is the root of a separable polynomial, hence, they are all contained in F_s.

Proposition 3.0.6. *Let F be a field and F_s the separable closure defined over an algebraic closure $\overline{F}$. Then $\overline{F} = F_s$ if and only if the field F is perfect.*

Proof. ($\Leftarrow$) If F is perfect, every irreducible polynomial in *F[x]* is then separable. Hence, if $\alpha \in \overline{F}$, let $f_\alpha \in F[x]$ be its minimum polynomial it is separable by hypothesis.

$$\Rightarrow \alpha \in F_s \Rightarrow \overline{F} \subset F_s$$

meaning that they are equal.
($\Rightarrow$) Let $f \in F[x]$ be an irreducible polynomial and $\alpha \in \overline{F}$ one of its roots. By hypothesis, $\alpha \in F_s$, hence its minimum polynomial p_α is separable, hence $p_\alpha | f$. But since f was irreducible by hypothesis, $f = p_\alpha$, so f is separable. □

Since the absolute Galois Groups that will be studied later on are both built over two perfect fields, we will give a brief example of a non-perfect field.

Example 3.0.7. Let $\mathbb{F}_p$ be the finite field of characteristic p, prime integer, and t a transcendental element over F. We prove that the transcendental extension $\mathbb{F}_p(t)$ is non-perfect. Let's consider the polynomial $f(x) := x^p - t \in \mathbb{F}_p(T)[X]$

1. f is irreducible thanks to Eisenstein's Criterion (the general one for UFDs). In fact, t is first of all prime in $\mathbb{F}_p(T)$, the polynomial is monic and the last coefficient is t itself, hence t^2 does not divide it.

2. f is totally inseparable. In an extension were α is a root for f then since the fundamental field has characteristic p, $f(x) = (x - \alpha)^p$

So in this case, $\mathbb{F}_p(T) \subset \mathbb{F}_p(T)_s \subset \overline{\mathbb{F}_p(T)}$. Specifically, we have that the algebraic extension associated with the polynomial $x^p - t$ is called *purely inseparable*. The first variation of Galois theory for some purely inseparable extensions was proposed in the 1940s and was updated during the 1970s. Despite their interest, such results are way too far from this paper's objective and so we are satisfied with just a practical example of a non-perfect field.

3.1 The Absolute Galois group of finite fields

Let p be a prime number and $F = \mathbb{F}_p$ be the finite field of order p. We already know that any finite Galois extension of $\mathbb{F}_p$ of order m is $\mathbb{F}_p$-isomorphic to the extension $\mathbb{F}_{p^m}/\mathbb{F}_p$ and it is specifically the splitting field of the polynomial $x^{p^m} - x$. Now, the Galois groups associated with an arbitrary extension $\mathbb{F}_{p^m}/\mathbb{F}_p$ is generated by the *Frobenius automorphism*, which is defined as

$$\sigma : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$$

$$\alpha \longmapsto \alpha^p$$

Furthermore, there is an isomorphism such that $\mathrm{Gal}(\mathbb{F}_p/\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z}$.

It follows from this that given a generic extension of the form $\mathbb{F}_{p^m}/\mathbb{F}_p$, all the possible intermediate extensions are all Galois and of the form $\mathbb{F}_{p^n}/\mathbb{F}_p$ where $n|m$. Consequentially we have the two following anti-isomorphic diagrams:

$$\begin{array}{c} \mathbb{F}_{p^m} \\ | \\ \mathbb{F}_{p^n} \\ | \\ \mathbb{F}_p \end{array} \qquad\qquad \begin{array}{c} \langle\sigma\rangle \simeq \mathbb{Z}/m\mathbb{Z} \\ | \\ \langle\sigma\rangle/\langle\sigma^n\rangle \simeq \mathbb{Z}/(m/n)\mathbb{Z} \\ | \\ \{1\} \end{array}$$

Thanks to this remark we know the entire structure of the lattice beneath the separable closure of a finite field of prime order p, but more importantly, we know that all the possible finite extensions are Galois. By what we have proven in Chapter 2 we have that the set of all normal subgroups of the Galois group is an inverse system when the morphism is the restriction map between the quotient groups. In this case the restriction map between the Galois groups of two extensions $\mathbb{F}_{p^n}/\mathbb{F}_p \subset \mathbb{F}_{p^m}/\mathbb{F}_p$, where $n|m$, sends the Frobenius automorphism to itself meaning that such restriction map

$$\Phi_{nm} : \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \longrightarrow \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$$

$$\tau \longmapsto \tau_{|\,\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)}$$

is the analogue of the reduction map mod n between $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. This implies that the inverse system defined by the normal subgroup of the absolute Galois group is precisely the same defined in the example 1.3.3. As proven in Chapter 2, we know that the Absolute Galois group $G_{\mathbb{F}_p}$ we are looking for is the profinite group obtained as the inverse limit of all finite Galois extensions of $\mathbb{F}_p$ contained in its separable closure. Thanks to the observations we just made all the possible Galois extensions are $\mathbb{F}_{p^n}$, $n \in \mathbb{N}$, hence:

$$G_{\mathbb{F}_p} = \varprojlim_{K/\mathbb{F}_p \text{ finite Galois}} \mathrm{Gal}(K/\mathbb{F}_p) = \varprojlim_{n} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$$

Remark. *The choice of p does not affect the result we just found. Meaning that regardless of which prime we use to define the finite field all the Absolute Galois groups are isomorphic to $\hat{\mathbb{Z}}$.*

3.2 The Absolute Galois group of $\mathbb{Q}_p$

The field of p-adic numbers was first described in 1897 by Kurt Hensel and since then they have been constantly studied because of their topological, metric and modular properties. The goal of this section is to study the basic properties of the set of p-adic numbers as well as its extensions in order to compute the Absolute Galois group, which is a process that is far from being trivial.

3.2.1 Discrete Valuation Rings & Absolute Values

Here below we will first introduce the analytic preliminaries and later on, the algebraic ones required for both the definition of $\mathbb{Q}_p$ and the study of p-adic extensions through a metric and an algebraic meaning.

Absolute values

Definition 3.2.1. Let F be a field.

1. An *absolute value* (also called *norm*) is a map, denoted $\|\cdot\|$, from F to non-negative real numbers such that:

   (a) $\|x\| = 0 \leftrightarrow x = 0$

   (b) $\|xy\| = \|x\|\|y\|$

   (c) $\|x + y\| \leq \|x\| + \|y\|$

   Regarding the last condition, a norm $\|\cdot\|$ on a field F is said to be *non-Archimedean* if the property $\|x + y\| \leq \max(\|x\|, \|y\|)$ always holds. Otherwise, it is called *Archimedean*.

2. The *metric induced by a norm* $\|\cdot\|$ is defined as $d(x, y) := \|x - y\|$

Example 3.2.2. Just to give a practical example, the usual norm on real numbers is Archimedean. We find a couple of numbers $x, y \in \mathbb{R}$ such that $|x + y| > \max(|x|, |y|)$. Such numbers are for example, $|1/2 + 1/3| = |5/6| = 5/6 > \max(|1/2|, |1/3|) = 1/2$.

Definition 3.2.3. Let $\|\cdot\|_1, \|\cdot\|_2$ be non-trivial absolute values of a field F. Then we say that they are equivalent if they induce the same topology on F. An equivalence class of absolute values on F is called a *place*.

A final, but fundamental aspect is the following:

Definition 3.2.4. Given a field F and an absolute value $|\cdot|$, we say that F is *complete*, with respect to $|\cdot|$, if every $|\cdot|$-Cauchy sequence converges in F in the metric induced by $|\cdot|$. If a field $(F, |\cdot|)$ is not complete then it can undergo the process of *completion* which is a process that adds to F every possible limit of every possible $|\cdot|$-Cauchy sequence of elements in F by defining equivalence classes of sequences that are equivalent if and only if they have the same limit, i.e. given two sequences $\{x_n\}_{n\in\mathbb{N}} \sim \{y_n\}_{n\in\mathbb{N}}$, they are equivalent if $\lim_{n\to\infty} |x_n - y_n| = 0$.

Remark. *The relation introduced in the previous definition is indeed an equivalence relation. Let's consider the $|\cdot|$-Cauchy sequences $\{a_i\}_{i\in\mathbb{N}}, \{b_i\}_{i\in\mathbb{N}}, \{c_i\}_{i\in\mathbb{N}}$*

- $|a_i - a_i| = 0 \Rightarrow \lim_{i\to\infty} |a_i - a_i| = 0$
- *If $\{a_i\}_{i\in\mathbb{N}} \sim \{b_i\}_{i\in\mathbb{N}}$, then $|b_i - a_i| = |a_i - b_i| \to_{i\to\infty} 0 \Rightarrow \{b_i\}_{i\in\mathbb{N}} \sim \{a_i\}_{i\in\mathbb{N}}$*
- *Given $\{a_i\}_{i\in\mathbb{N}} \sim \{b_i\}_{i\in\mathbb{N}}, \{b_i\}_{i\in\mathbb{N}} \sim \{c_i\}_{i\in\mathbb{N}}$, then*

$$|a_i - c_i| = |a_i - b_i + b_i - c_i| \leq |a_i - b_i| + |b_i - c_i| \to_{i\to\infty} 0$$

hence $\{a_i\}_{i\in\mathbb{N}} \sim \{c_i\}_{i\in\mathbb{N}}$

Discrete Valuation Rings & Valuations

In order to associate the metric preliminaries to an algebraic point of view we will need to briefly recall some basic algebraic concepts. A non-empty set R with two binary operations $+, \cdot$, called respectively *addition* and *multiplication*, is called a *ring*, if $(R, +)$ is an abelian group and if the multiplication $\cdot$ is associative, with an identity element and distributive with respect to addition. Since the family of rings is quite wide, from now on we will work specifically with a family of rings called *commutative integral domains*, which are such that the multiplication is commutative and the product of two nonzero elements is nonzero.

Definition 3.2.5. A subset I of a ring R is called an *ideal* if $(I, +)$ is a subgroup of $(R, +)$ and if it is such that for every choice of elements $i \in I, s \in R$, then $i \cdot s \in I$.

An ideal $I \subset R$ is *proper* if $I \neq R$ and it is a *maximal ideal* if proper and not contained in a larger proper ideal. An arbitrary ring R is consequentially called *local* if it has a unique maximal ideal $\mathfrak{m}$.

Lemma 3.2.6. *1. If R is a local ring, then its maximal ideal is $\mathfrak{m} = R/R^\times$;*

2. If $R/R^\times$ is an ideal, it is maximal and R is a local ring.

Proof. Let's first note that every proper ideal $I \subset R$ is also a subset for $R/R^\times$. If there exists an element $x \in R^\times \cap I$, then $xR \subset I \Rightarrow I = R$, contradicting properness.

1. Suppose R local. It is known that $\mathfrak{m} \subset R/R^\times$. If $\mathfrak{m} \neq R/R^\times$, then there exists $y \in R/R^\times$ such that $y \notin \mathfrak{m}$. But then y must be contained in a maximal ideal $\mathfrak{m}'$ not equal to $\mathfrak{m}$, which leads to a contradiction.

2. By the above arguments $R/R^\times$ must be maximal. Moreover, it also contains any proper ideal of R, so it must be the unique maximal ideal. Hence, R is local.

□

Definition 3.2.7. A ring R is a *discrete valuation ring* (DVR), if:

1. R is a local ring, and
2. R is a PID (Principal Ideal Domain), and
3. R is *not* a field.

Definition 3.2.8. If R is a DVR, then its unique maximal ideal $\mathfrak{m}$ is principal and any generator of $\mathfrak{m}$ is called a *uniformiser*. Such uniformiser is usually labeled with π.

Proposition 3.2.9 ([9], p. 40-41)**.** *Let R be a DVR with uniformiser π. Let $F = \mathrm{Frac}(R)$ (fraction field of R), then every element in F can be written uniquely in the form $x = u\pi^r$ where $u \in R^\times, r \in \mathbb{Z}$.*

The reason why we defined both the DVRs in the first place and the uniformiser it is because they are deeply connected with a family of field functions:

Definition 3.2.10. A *valuation* on a field F is a function

$$v : F^\times \to \mathbb{R}$$

such that for all $x, y \in F^\times$:

1. $v(xy) = v(x) + v(y)$
2. $v(x + y) \leq \min(v(x), v(y))$

Remark. *Following from the definition, we can easily prove that $v(1) = 0$ and $v(x) = -v(x^{-1})$. In fact, $v(1) = v(1 \cdot 1) = v(1) + v(1) = 2v(1)$. Hence, since we are working integral domains, $v(1) = 0$. Following from this, $0 = v(1) = v(x \cdot x^{-1}) = v(x) + v(x^{-1})$.*

It is important to notice that a valuation is not always a surjection, for instance, the valuation's codomain could be $\mathbb{Z}$ instead of $\mathbb{R}$, the first one being a discrete set and the second one not. Such situations are not uncommon and for this, we give the following classification:

Definition 3.2.11. Given a field F and a valuation v then v is a *discrete valuation* if the subset $v(F^\times) \subset \mathbb{R}$ is discrete. In particular, if $v(F^\times) = \mathbb{Z}$ then it is also said to be *normalized*.

Definition 3.2.12. If v is a valuation on a field F, with the associated absolute value $|\cdot|$, we define:

1. $\mathcal{O} := \{x \in F | |x| \leq 1\} = \{x \in F | v(x) \geq 0\}$, the *valuation ring*;
2. $\mathfrak{m} := \{x \in F | |x| < 1\} = \{x \in F | v(x) > 0\}$, the *maximal ideal*;
3. $k := \mathcal{O}/\mathfrak{m}$, the *residue field*.

Now, with the definition of a discrete valuation, it is possible to explain their correlation with DVRs.

Lemma 3.2.13. *If F is a field with a non-trivial discrete valuation v, then its valuation ring $\mathcal{O}$ is a DVR. Conversely, if R is a DVR, then there exists a unique normalized discrete valuation v on* $\mathrm{Frac}(R)$ *such that R is its valuation ring.*

Proof. We must prove that $\mathcal{O}$ respects the conditions in Definition 3.2.7.

1. Note that $\mathfrak{m} = \mathcal{O}/\mathcal{O}^\times$ and it is an ideal. Hence, thanks to Lemma 3.2.6, $\mathcal{O}$ is local;
2. Let $I \subset \mathcal{O}$ be a non-zero ideal. Let $a \in I$ such that $v(a) = \min\{v(x) | x \in I\} \subset \mathbb{R}_{\geq 0}$. Since v is discrete, this minimum is always attained. Now, if $x \in I$, then $v(x) \geq v(a)$, so $x\mathcal{O} \subset a\mathcal{O} \Rightarrow I \subset a\mathcal{O}$, but it is also true that $a\mathcal{O} \subset I$, hence, $I = a\mathcal{O}$;
3. Since v is non-trivial, there exists an element $x \in \mathcal{O}$ such that $v(x) \neq 0 \Rightarrow v(x) \notin \mathcal{O}$. Hence, $\mathcal{O}$ is not a field.

Conversely, let π be a uniformiser in F, consequentially every $x \in F^\times$ can be written uniquely as $x = u\pi^r$. We define

$$\begin{aligned} v \colon F^\times &\longrightarrow \mathbb{Z} \\ u\pi^r &\longmapsto r \end{aligned}$$

Note that $v(x) \geq 0 \leftrightarrow r \geq 0 \leftrightarrow r \in R$, so $R = \mathcal{O}$. □

Finally, the most important result that put together valuations and the previously introduced absolute values is the following:

Lemma 3.2.14. *Let $0 < a < 1$ be a fixed real number.*

1. *If v is a valuation over a field F, then the function*

$$\begin{aligned} |\cdot|_v \colon F &\longrightarrow \mathbb{R}_{\geq 0} \\ x &\longmapsto a^{v(x)} \end{aligned}$$

   is a non-Archimedean absolute value on F. We use the convention that for $x = 0$ the valuation is equal to ∞.

2. *If $|\cdot|$ is a non-Archimedean absolute value on F, then the function*

$$\begin{aligned} v_{|\cdot|} \colon F^\times &\longrightarrow \mathbb{R} \\ x &\longmapsto \log_a |x| \end{aligned}$$

   is a valuation on F.

Proof. To prove both facts it is only necessary to show that the definitions for a valuation and an absolute value hold for v and $|\cdot|$ respectively.

1. Let's fix $x, y \in F$.

   - $|x|_v = 0 \leftrightarrow a^{v(x)} = 0$. If $v(x) \in \mathbb{R}$ this is not possible, hence $x = 0$.
   - $|xy|_v = a^{v(xy)} = a^{v(x)+v(y)} = a^{v(x)}a^{v(y)} = |x|_v|y|_v$
   - $|x+y|_v = |a^{v(x+y)}|$. By definition we have that $v(x+y) \geq \min(v(x), v(y))$, so $a^{v(x+y)} \leq a^{\min(v(x),v(y))}$ since $f(x) = a^x, a \in (0,1)$ is monotonically non-increasing. Hence, $|x+y|_v \leq \max(|x|_v, |y|_v) \leq |x|_v + |y|_v$. Thanks to this chain of inequalities we have also proved that $|\cdot|_v$ is non-Archimedean.

2. Let's fix $x, y \in F^\times$.

   - $v_{|\cdot|}(xy) = \log_a(|xy|) = \log_a(|x||y|) = \log_a(|x|) + \log_a(|y|) = v_{|\cdot|}(x) + v_{|\cdot|}(y)$
   - $v_{|\cdot|}(x+y) = \log_a(|x+y|)$. Since $|\cdot|$ is non-Archimedean and $\log_a(\cdot)$ is monotonically non-increasing:

     $$v_{|\cdot|}(x+y) \geq \log_a(\max(|x|,|y|)) = \min(\log_a(|x|), \log_a(|y|)) = \min(v_{|\cdot|}(x), v_{|\cdot|}(y))$$

□

Not only this lemma explicitly tells us how to associate a valuation with an absolute value and vice versa, but it also shows that all such obtainable norms are non-Archimedean.

3.2.2 The *p*-adic numbers

The set of p-adic numbers is related to rational numbers and in order to properly define it, we will need to focus on a specific norm:

Proposition 3.2.15. *Let p be any prime number, then the following map:*

$$|x|_p = \begin{cases} 1/p^{\mathrm{ord}_p x} & \text{if } x \neq 0 \\ 0 & \text{otherwise} \end{cases} \tag{3.1}$$

where $\mathrm{ord}_p x$ is the highest power of p which divides x, is a norm on $\mathbb{Q}$, called p-adic norm

Proof. We prove that every property in Definition 3.2.1 holds for $|\cdot|_p$.

- If $x = 0 \Rightarrow |x|_p = 0$ by definition. Conversely, if $|x|_p = 0$ it is not possible that $x \neq 0$, because otherwise x would be such that $1/p^{\mathrm{ord}_p x} = 0$ which is impossible;
- Let's consider $x, y \in \mathbb{Q}/\{0\}$, then they can both be written as $x = p^{\mathrm{ord}_p(x)}a_x/b_x$ and $y = p^{\mathrm{ord}_p(y)}a_y/b_y$, where a_x, b_x, a_y, b_y are not divided by p. Then:

  $$xy = p^{\mathrm{ord}_p(x)+\mathrm{ord}_p(y)}(a_x a_y)/(b_x b_y)$$
  $$\Rightarrow |xy|_p = 1/p^{\mathrm{ord}_p(xy)} = 1/p^{\mathrm{ord}_p(x)+\mathrm{ord}_p(y)} = 1/p^{\mathrm{ord}_p(x)} 1/p^{\mathrm{ord}_p(y)} = |x|_p|y|_p.$$

  If at least one between x, y is equal to 0, then the property trivially holds;

- Let's consider $x, y \in \mathbb{Q}/\{0\}$ and use the notation introduced in the previous point. Let's suppose that $\mathrm{ord}_p(x) \leq \mathrm{ord}_p(y)$, then

$$|x+y|_p = |p^{\mathrm{ord}_p(x)} a_x/b_x + p^{\mathrm{ord}_p(y)} a_y/b_y|_p = |p^{\mathrm{ord}_p(x)}(a_x/b_x + p^{\mathrm{ord}_p(y)-\mathrm{ord}_p(x)} a_y/b_y)|_p$$

  By hypothesis, a_x, b_x are not divided by p, hence,

$$|x+y|_p \leq 1/p^{\mathrm{ord}_p(x)} \leq 1/p^{\mathrm{ord}_p(x)} + 1/p^{\mathrm{ord}_p(y)} = |x|_p + |y|_p$$

  If at least one between x, y is equal to 0, then the property trivially holds;

□

Remark. *What is interesting and fundamental about this norm, is that $|\cdot|_p$ is non-Archimedean. The reason for this is explicit in the proof of the previous proposition when the property of subadditivity was being proven.*

Now, a quite renowned result of measure theory tells us that every non-trivial norm over real numbers is equivalent to one another, hence the only place for non-trivial norms has the Euclidian one as a representative. Does this also apply to rational numbers? The answer is no, but it is not so far from reality.

Theorem 3.2.16. *(Ostrowski) [[9], p. 28-30] Any non-trivial absolute value $|\cdot|$ on $\mathbb{Q}$ is equivalent to either the standard norm $|\cdot|$ or $|\cdot|_p$ for a prime p. Moreover, the completion of a number field F with respect to an Archimedean absolute value $|\cdot|$ is always isomorphic to $\mathbb{R}$ or $\mathbb{C}$ as topological fields.*

This means that when working with rational numbers absolute values are really limited and this limitation is the reason why p-adic numbers are such a powerful resource in algebra even if we will have only a small taste of such power. With this in mind, we now properly build the p-adic numbers.

The construction of $\mathbb{Q}_p$

From now on p will be considered as a fixed finite prime number.

What's the idea behind p-adic numbers? By recalling Theorem 3.2.16 we can see that when a field is completed with respect to an Archimedean norm, the resulting field is isomorphic to real numbers or complex numbers, but for what concerns rational numbers, the process of completion, if done with respect to the usual norm $|\cdot|$, precisely results in obtaining the set of real numbers. We might want to see what could happen if the completion was made with respect to a non-Archimedean norm and since we already know an example of such a norm we define the following set:

Definition 3.2.17. The set of *p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Now, since we have already stated and defined the metric completion of a field, this definition might be enough, but for the sake of formality, we will still go through the process of completion so that we explicitly show which are the elements of $\mathbb{Q}_p$ obtained. For this matter, let S be the set of rational $|\cdot|_p$-Cauchy sequences and let's define the following equivalence $\sim$: two sequences of S, $\{a_i\}_{i\in\mathbb{N}}, \{b_i\}_{i\in\mathbb{N}}$, are equivalent if and only if $|a_i - b_i|_p \to_{i\to\infty} 0$.

Now that we have equivalence classes, we also want to extend the definition of the p-adic norm for these as well. Let $a \in S/\sim$ be an equivalence class and $\{a_i\}_{i\in\mathbb{N}}$ one of its representatives, then we define $|a|_p := lim_{i\to\infty}|a_i|_p$.

Remark. *The limit always exists. Since for a=0 this is trivial, we prove it for $a \neq 0$. If a is not 0 then for some ϵ and $\forall N \exists i_N > N$ such that $|a_{i_N}|_p > \epsilon$. If we choose N large enough so that $|a_i - a_j|_p < \epsilon$ when $i, j > N$, we have $|a_i - a_{i_N}|_p < \epsilon \forall i > N$. Since $|a_{i_N}|_p > \epsilon$, it follows that $|a_{i_N}|_p = |a_i|_p$. Thus, this value is constant for all $i > N$, hence, its value is the value of the limit.*

Now we have a more accurate description of the set we introduced and we can upgrade its definition:

Definition 3.2.18. For every positive finite prime p, the *p-adic numbers* are the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$, that is:

$$\mathbb{Q}_p := \{|\cdot|_p\text{-Cauchy sequences in } \mathbb{Q}\}/\sim$$

Now, it is important to notice that the structure we have obtained has two important properties:

1. $\mathbb{Q}_p$ is a field, $(\mathbb{Q}_p, +, \cdot, \{0\}, \{1\})$, where $+$ and $\cdot$ are defined as follows:

$$\begin{aligned} +\colon\ \mathbb{Q}_p \times \mathbb{Q}_p &\longrightarrow \mathbb{Q}_p \\ (\{a_i\}, \{b_i\}) &\longmapsto \{a_i + b_i\} \end{aligned}$$

$$\begin{aligned} \cdot\colon\ \mathbb{Q}_p \times \mathbb{Q}_p &\longrightarrow \mathbb{Q}_p \\ (\{a_i\}, \{b_i\}) &\longmapsto \{a_i b_i\} \end{aligned}$$

2. $\mathbb{Q}$ is strictly contained in $\mathbb{Q}_p$, this is because there exists a correspondence between a rational number q and the constant sequence of value q. This fact also tell us that the char($\mathbb{Q}_p$) is 0, hence it is a perfect field; Moreover, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ by definition.

We now prove that the operations are well-defined and that they really induce a field structure. First of all, given an equivalence class $a \neq 0$ we define its (multiplication and bilateral) inverse as $a^{-1} := \{1/a_i\}_{i\in\mathbb{N}}$ where $\{a_i\}_{i\in N}$ is a representative of a and $-a := \{-a_i\}_{i\in N}$ as its additive inverse. Let's consider two equivalence classes a, b and two sequence couples $(\{a_i\}, \{b_i\}), (\{a'_i\}, \{b'_i\})$ such that both are representatives of the couple (a, b).

1. $|a_ib_i - a'_ib'_i|_p = |a'_i(b'_i - b_i) + b_i(a'_i - a_i)|_p \leq \max(|a'_i(b'_i - b_i)|_p, |b_i(a'_i - a_i)|_p)$ and as $i \to \infty$ we have that $lim_{i\to\infty}|a_ib_i - a'_ib'_i|_p \leq 0$ hence the two are equivalent.

2. $|a_i + b_i - (a'_i + b'_i)|_p = |(a_i - a'_i) + (b_i - b'_i)|_p \leq |a_i - a'_i|_p + |b_i - b'_i|_p$ and as $i \to \infty$ both $|a_i - a'_i|_p, |b_i - b'_i|_p \to 0$

With the same proof strategy, we can easily show that both $+$ and $\cdot$ are associative and commutative, having respectively the classes $\{0\}$ and $\{1\}$ as bilateral identity elements. Finally, distributively also holds between multiplication and addition.
Now, recalling Lemma 3.2.14, we know that the p-adic norm $|\cdot|_p$ induces a valuation function over $\mathbb{Q}$. Specifically, such valuation is defined as $v(x) = \log_a(|x|_p) = -\log_a(p^{\mathrm{ord}_p(x)})$, where a is a fixed positive number smaller than 1 and since for every prime $p, 1/p < 1$ we can choose $a = 1/p$. This way, $v(x) = \mathrm{ord}_p(x)$ and it is called the *p-adic valuation*. Being such an important map, v_p has an alternative definition, in which rational numbers are represented as $p^n a/b$ where p does not divide either a and b:

$$v_p: \quad \mathbb{Q}^\times \longrightarrow \mathbb{Z}$$

$$\alpha = p^n a/b \longmapsto n$$

It is easy to notice that the ord operator makes the p-adic valuation a normalized discrete valuation. Recalling the subsets defined in Definition 3.2.12, in the specific case of $\mathbb{Q}_p$, the valuation ring for the p-adic valuation is called $\mathbb{Z}_p$: the *p-adic integers*. Consequentially, the maximal ideal is $p\mathbb{Z}_p$ and the residue field $k = \mathbb{Z}_p/p\mathbb{Z}_p$. This also tells us that a uniformiser for $\mathbb{Q}_p$ is p itself.

Remark. *Similarly to $\mathbb{Q}_p$, the set of integers $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. In fact, we prove that the set $\mathbb{Q} \cap \mathbb{Z}_p$, written usually as $\mathbb{Z}_{(p)}$, is dense in $\mathbb{Z}_p$ and $\mathbb{Z}$ is dense $\mathbb{Z}_{(p)}$.*

1. *Let $a/b \in \mathbb{Z}_{(p)}$. Since b is prime to p, for each $n \geq 1$ we may choose a sequence $y_n \in \mathbb{Z}$ such that $by_n \equiv 1 \mod p^n$. Hence, $\{y_n\}_{n\in N}$ is a $|\cdot|_p-$Cauchy sequence of integers tending to $1/b$, and so ay_n tends to a/b. Hence, $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$;*

2. *Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ by definition, then the set $\mathbb{Q} \cap \mathbb{Z}_p$ is dense in the induced subspace topology.*

Lemma 3.2.19. $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$

Proof. We prove that since $\mathbb{Z} \subset \mathbb{Z}_p$, there is an isomorphism between $\mathbb{Z}_p/p\mathbb{Z}_p$ and $\mathbb{Z}/p\mathbb{Z}$. Consider the projection

$$\pi: \quad \mathbb{Z}_p \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

$$\textstyle\sum_{n=0}^{\infty} a_n p^n \longmapsto a_0$$

To have proof of the fact that π is a homomorphism, refer to [[10], p.27]. Let $a \in \ker(\pi)$, then $\pi(a) = 0 \leftrightarrow a_0 = 0 \leftrightarrow p|a \leftrightarrow a \in p\mathbb{Z}_p$. We conclude with the Isomorphism Theorem. □

What's most interesting about p-adic integers is that their structure is not only given by the p-adic valuation, but it also has a more topological structure. First of all, similar to integers $\mathbb{Z}$ the ideals of $\mathbb{Z}_p$ are all and only the ones of the form $\mathbb{Z}_p/p^n\mathbb{Z}_p, n \in \mathbb{N}$. Let's recall Lemma 3.2.13, we have shown in the proof that the valuation ring for a discrete valuation is a PID, hence given an ideal I we have a p-adic integer a such that $a\mathbb{Z}_p = I$. Thanks to the fact that $a = p^{\mathrm{ord}_p(a)} \sum_{n=0}^{\infty} a_n p^n$, it is automatic that $I = p^{\mathrm{ord}_p(a)}\mathbb{Z}_p$. Hence all possible ideals for $\mathbb{Z}_p$ are of the form $p^k\mathbb{Z}_p$ for every $k \in \mathbb{N}$.

Lemma 3.2.20. $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}, n \geq 1$

Proof. We have already proven the case for $n = 1$. We use the reduction homomorphism between $\mathbb{Z}$ and $\mathbb{Z}_p/p^n\mathbb{Z}_p$ that for every integer $x \mapsto x \mod p^n\mathbb{Z}_p$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ then for every $x \in \mathbb{Z}_p$, there exists $a \in \mathbb{Z}$ such that $|a - x|_p < 1/p^n$, this means consequentially that $x \equiv a \mod p^n\mathbb{Z}_p$ and that the morphism is a surjection. Now we compute the kernel of this map. Let $x \in \mathbb{Z}$ such that $x \equiv 0 \mod p^n\mathbb{Z}_n$, but this happens if and only if $p^n|x$, so $\ker = p^n\mathbb{Z}$. Thanks to the First Homomorphism Theorem $\mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$. □

Thanks to this correspondence, we can state that $\{\mathbb{Z}_p/p^n\mathbb{Z}_p\}_{n\in\mathbb{N}}$ is indeed an inverse system thanks to the fact that $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n\in\mathbb{N}}$ is an inverse system with reduction morphisms. Moreover, thanks to what we learned in Chapter 1 we know that consequentially the p-adic integers are themselves the inverse limit, hence, $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

At this point, we have introduced $\mathbb{Q}_p$ and also talked about the subring $\mathbb{Z}_p$, but we have yet to talk about its extensions. Some may ask themselves: "What might happen when $\mathbb{Q}_p$ is extended? What happens to the p-adic norm?". The answer is quite surprising. In reality, when given any number field F, a similar non-Archimedean $\mathfrak{p}$-*adic absolute value* can always be defined and it is in fact a generalization of the $|\cdot|_p$ where $\mathfrak{p} \subset K$ is a *prime ideal*, specifically, a proper ideal such that if the product of two elements $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}$. The following theorem is consequentially an important result for p-adic extensions:

Theorem 3.2.21 ([9], p. 31)**.** *Given a field F and a norm $|\cdot|_{\mathfrak{p}}$, if the completion of F with respect to such norm is labelled as $F_{\mathfrak{p}}$, then the extension $F_{\mathfrak{p}}/\mathbb{Q}_p$ is a finite field extension of degree at most $[F : \mathbb{Q}]$ and the restriction of $|\cdot|_{\mathfrak{p}}$ to $\mathbb{Q}$ is equal to $|\cdot|_p$*

On the other hand, is also possible to extend the p-adic norm onto a field F if a finite extension of $\mathbb{Q}_p$.

Lemma 3.2.22. *Let F be a finite extension of $\mathbb{Q}_p$, then the residue field k_F is isomorphic to a finite field $\mathbb{F}_{p^n}$ for some $n \in \mathbb{N}$.*

Proof. We prove that the residue field for F is a finite field extension of the residue field $k_{\mathbb{Q}_p}$ for $\mathbb{Q}_p$. Since such residue field is isomorphic to $\mathbb{F}_p$, we would consequentially have that $k_F \simeq \mathbb{F}_{p^n}$. By definition, $k_F = \mathcal{O}_F/\mathfrak{m}_F$ and by Theorem 3.2.21 we know that such norm extends the p-adic norm in $\mathbb{Q}_p$. Hence, given an element $x \in k_{\mathbb{Q}_p}$, then $1 > |x|_p = |x|_{\mathfrak{p}} \Rightarrow x \in k_F$. Hence, $k_{\mathbb{Q}_p} \subset k_F$, meaning it is indeed a field extension. □

3.2.3 Some tools from Ramification Theory

Let's consider two fields L/F, both finite extensions of $\mathbb{Q}_p$, with valuation rings $\mathcal{O}_{L(resp.F)}$, uniformisers $\pi_{L(resp.F)}$, normalized discrete valuations $v_{L(resp.F)}$ and residue fields $k_{L(resp.F)}$.

Definition 3.2.23. The *ramification index* of L/F is $e(L/F) := v_L(\pi_F) \in \mathbb{Z}$. The *residue index* of L/F is $f(L/F) := [k_L : k_F] \in \mathbb{Z} \cup \{\infty\}$

And the important property that these two indexes have is the following:

Lemma 3.2.24 ([9], p.101-102)**.** *For a finite extension L/F the degree $[L : F] = e(L/F)f(L/F)$*

In addition, the ramification index is used to classify extensions in the following meaning:

Definition 3.2.25. The extension L/F is:

1. *unramified* if $e(L/F) = 1$
2. *ramified* if $e(L/F) > 1$
3. *totally ramified* if $e(L/F) = [L : F]$

The reason why we introduced this classification is mainly because of the next theorem, which gives an interesting result about the possible subfields of the extension L/F.

Theorem 3.2.26 ([9], p.114)**.** *Let L/F be a finite extension, with residue fields respectively $\mathbb{F}_{q^n}, \mathbb{F}_q$. Let $m := q^n - 1$ and ζ_m be a primitive mth root of 1. Then $F \subset F(\zeta_m) \subset L$, with*

$$F(\zeta_m)/F \text{ unramified}$$

$$L/F(\zeta_m) \text{ totally ramified}$$

The following set gives the last piece of our puzzle:

Definition 3.2.27. Let L/F be a Galois extension and let's consider the reduction map between $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(k_L/k_F)$, then we call *inertia group* the kernel of such map.

$$I_{L/F} := \ker[\mathrm{Gal}(L/F) \to \mathrm{Gal}(k_L/k_F)]$$

As the kernel of a group homomorphism, the inertia group is a normal subgroup of the Galois group $\mathrm{Gal}(L/F)$, but since the reduction map is a surjection, we have that $|I_{L/F}| = |\mathrm{Gal}(L/F)|/|\mathrm{Gal}(k_L/k_F)| = e(L/F)$.

Let's now consider the easy case where $F = \mathbb{Q}_p$, hence L is consequentially a finite extension of $\mathbb{Q}_p$. Recalling Lemma 3.2.22 and Definition 3.2.23 we can clearly say that L's residue field is isomorphic to $\mathbb{F}_{p^{f(L/\mathbb{Q}_p)}}$ and we proceed to study the Galois groups of $L/\mathbb{Q}_p(\zeta_m)$ and $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$, where $m := p^{f(L/\mathbb{Q}_p)} - 1$. To make everything easier $n := f(L/\mathbb{Q}_p)$.

1. $\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p)$ is isomorphic to $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. This is thanks to the reduction map $\phi : \sigma \mapsto \sigma \mod \pi$, where π is a uniformiser in $\mathbb{Q}_p(\zeta_m)$.

- The fact that such map is an injection is claimed on page 114 ([9]) in the proof of the analog of Theorem 3.2.26;
- It is a surjection by counting size. First of all, since $L/\mathbb{Q}_p(\zeta_m)$ is totally ramified its residue index $f(L/\mathbb{Q}_p(\zeta_m)) = 1$, but since $[k_L : k_{\mathbb{Q}_p(\zeta_m)}] = f(L/\mathbb{Q}_p(\zeta_m))$ we have that L and $\mathbb{Q}_p(\zeta_m)$ have the same residue field. Having this:

  $$e(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p)f(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = [\mathbb{Q}_p(\zeta_m) : \mathbb{Q}_p] \leq [k_{\mathbb{Q}_p(\zeta_m)} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$$

  Having that $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is unramified:

  $$\begin{aligned} &e(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = 1 \\ &\quad \Rightarrow n = f(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = [\mathbb{Q}_p(\zeta_m) : \mathbb{Q}_p] \leq [k_{\mathbb{Q}_p(\zeta_m)} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n \end{aligned}$$

  Hence, $\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \simeq \mathbb{Z}/n\mathbb{Z}$

2. As for the second group, we have that $\mathrm{Gal}(L/\mathbb{Q}_p(\zeta_m)) \simeq I_{L/\mathbb{Q}_p}$. Following from its definition, the inertia group $I_{L/\mathbb{Q}_p} = \ker[\mathrm{Gal}(L/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)]$ is a normal subgroup of $\mathrm{Gal}(L/\mathbb{Q}_p)$, and because of the Fundamental Theorem there exists a finite Galois extension K of F such that $I_{L/\mathbb{Q}_p} = \mathrm{Gal}(L/K)$:

   $$\{1\} \longrightarrow I(L/\mathbb{Q}_p) = \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(k_L/\mathbb{F}_p)$$

   Given the fact that $n = |\mathrm{Gal}(k_L/\mathbb{F}_p)| = f(k_L/\mathbb{F}_p)$, we have that $[L : \mathbb{Q}_p(\zeta_m)] = [L : \mathbb{Q}_p]/[\mathbb{Q}_p(\zeta_m) : \mathbb{Q}_p] = e(L/\mathbb{Q}_p)n/n = e(L/\mathbb{Q}_p)$. By adding this last result with Definition 3.2.27, we have that $|I_{L/\mathbb{Q}_p}|$ and $|\mathrm{Gal}(\Omega/\mathbb{Q}_p(\zeta_m))|$ are both equal to $e(L/\mathbb{Q}_p)$. As stated earlier, these two groups are actually isomorphic and to have an elegant and immediate proof of this fact refer to [11], page 7.

3.2.4 The structure of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$

Having all the necessary preliminaries, we are finally ready to present the structure of the absolute Galois Group of the p-adic numbers. As seen in Chapter 2, all Galois groups are profinite groups, and more specifically they are the inverse limit running over the quotients by normal subgroups. Since we are talking about Galois extension, all the normal subgroups of the absolute Galois group are all and only finite Galois extensions of p-adic numbers.

So the absolute Galois group of p-adic numbers is $G_{\mathbb{Q}_p} := \varprojlim_{L/\mathbb{Q}_p \text{finite Galois}} \mathrm{Gal}(L/\mathbb{Q}_p)$

We have already proven in Theorem 3.2.26 that all the extensions of $\mathbb{Q}_p$ can be broken into an unramified and a ramified part. Let's now fix the proper $m \in \mathbb{Z}$ and let ζ_m be the m-primitive root of the identity such that the two extensions $L/\mathbb{Q}_p(\zeta_m)$ and $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ are respectively totally ramified and unramified, then the Galois groups for this two extensions are well known: $\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p)$ is a finite cyclic group $\mathbb{Z}/n\mathbb{Z}$, for some n, and $\mathrm{Gal}(L/\mathbb{Q}_p(\zeta_m)) \backsimeq I_{L/\mathbb{Q}_p}$, hence we have that:

$$\mathrm{Gal}(L/\mathbb{Q}_p) \backsimeq \mathbb{Z}/n\mathbb{Z} \rtimes I_{L/\mathbb{Q}_p}$$

Morally, the Galois group of a finite Galois extension $\mathrm{Gal}(L/\mathbb{Q}_p)$ is composed of a cyclic unramified part and a ramified part. Passing to the inverse limit, we get:

$$G_{\mathbb{Q}_p} := [\varprojlim_{n} \mathbb{Z}/n\mathbb{Z}] \rtimes [\varprojlim_{L/\mathbb{Q}_p \text{ finite Galois}} I_{L/\mathbb{Q}_p}] = \hat{\mathbb{Z}} \rtimes I_{\mathbb{Q}_p}$$

It is interesting to notice that since the residue fields are always finite fields then the Absolute Galois group obtained in section 3.1 appears in the p-adic one as well. So, as stated at the beginning of the chapter, even if the two fields have completely different properties their Absolute Galois groups differ for only the inertia group.

Appendix A

Finite Galois Theory

Here below we will resume some of the important results and basic definitions known for finite Galois Theory that have been used throughout the paper

A.1 Field Extensions

Definition A.1.1. Let F and Ω be fields, Ω is called an *extension* of F if Ω contains F. Written Ω/F

An extension Ω/F is naturally an F-vector space and its dimension $dim_F\Omega = [\Omega : F]$ is called the *degree* of the extension, which is positive by definition. More specifically, if the degree is a finite integer then the extension is said to be *finite*.
Let Ω/F be an extension and $\alpha \in \Omega$, we define the following map:

$$ev_\alpha : F[x] \longrightarrow \Omega$$

$$f(x) \longmapsto f(\alpha)$$

called *evaluation*. This function is more precisely a ring homomorphism and it gives crucial information regarding the nature of α:

1. If $\ker(ev_\alpha) = \{0\}$ then α is said to be *transcendental* over F;
2. If $\ker(ev_\alpha) \neq \{0\}$ then α is said to be *algebraic* over F. Please note that since the kernel of a ring homomorphism is an ideal and $F[x]$ is a PID (Principle Ideals Domain) the subring $\ker(ev_\alpha) = (p)$, for a certain irreducible $p \in F[x]$ (supposed monic since F is a field by assumption) called *minimal polynomial*.

Remark. *Let's denote $F[\alpha] = Im(ev_\alpha)$, the smallest subring containing F and α and also a domain in Ω, thanks to the First Homomorphism Theorem we can assert that $F[x]/(p) \backsimeq F[\alpha]$, but a subring of a ring is a domain if and only if p is prime and consequentially irreducible. This also implies that $F[\alpha]$ is a subfield and will be denoted by $F(\alpha)$.*

Definition A.1.2. An extension Ω/F is said *algebraic* if every single element of Ω is algebraic over F, in particular, it is also said *simple* if there exists a specific element α such that $\Omega = F(\alpha)$. On the contrary, if there is at least one element in Ω that is not algebraic, then Ω/F is called *transcendental*.

A.2 Polynomials and field extensions

We have shown that field extensions are closely related to roots of polynomials and here we will summarize the correspondence between the two concepts. Let F be a field and Ω/F an extension.

Definition A.2.1. A polynomial $f \in F[x]$ *splits* in Ω if there exists a finite set of elements $\{a, a_1, ..., a_n\} \subset \Omega$ such that:

$$f(x) = a\prod_{i=1}^{n}(x - a_i), \exists a \in \Omega$$

Particularly, if there exist two different indexes i and j such that $a_i = a_j$ then the root a_i is called *multiple*. On the other hand, if f is such that for every extension of F where f splits, the set $a_1, ..., a_n$ has always n distinct elements, then f is called *separable* over F.

Definition A.2.2. With the notation above, if $\Omega = F(a_1, ..., a_n)$ then it is called *splitting field* for f over F.

Definition A.2.3. Ω/F is said to be a *separable* extension if it is a field extension and is such that for every $\alpha \in \Omega$ its minimal polynomial is separable over F.
Also, Ω/F is called *normal* if for every polynomial $f \in F[x]$ the following proposition holds:

$$\text{If } \exists\alpha \in \Omega \text{ such that } f(\alpha) = 0 \Rightarrow f \text{ splits in } \Omega$$

The following is a criterion for irreducible polynomials which is usually given for integers, but the generalization is also a useful result.

Lemma A.2.4. *(Generalized Eisentein's Criterion) Given an integral domain R, let $Q = \sum_{i=0}^{n} a_i x^i$ an element of $D[X]$. Suppose there exists a prime ideal $\mathfrak{p} \subset D$ such that:*

- $a_i \in \mathfrak{p}, \forall i \neq n$
- $a_n \notin \mathfrak{p}$
- $a_0 \notin \mathfrak{p}^2$

Then Q is irreducible in $D[X]$.

A.3 *F*-Automorphisms

Definition A.3.1. Let Ω/F be a field extension and $\sigma : \Omega \to \Omega$ a function. σ is said to be an *F-automorphism* if it is an isomoprhism such that $\sigma|_F \equiv id_F$. The set of all *F-automorphisms* is denoted by $\mathrm{Aut}(\Omega/F)$.

Proposition A.3.2. *Let $f(x) \in F[X]$ and R be the set of all roots of f in an appropriate extension. Let also Ω/F be the extension obtained by adding some of the roots in R to F: $\Omega = F(\alpha_1, ..., \alpha_r)$, for some $\alpha_1, ..., \alpha_r \in R$. Let now L/F be another extension such that L is a splitting field for f. Then:*

1. *The number of F-homomorphisms between L and Ω is at most $[L : F]$ and is exactly $[L : F]$ if f has only distinct roots in L*
2. *If Ω is also a splitting field for f then every F-homomorphism is also an F-isomorphism*

Corollary A.3.3. *Let $f \in F[X]$ be a separable polynomial, then for every couple of splitting fields for f L, Ω, there exists an F-isomorphism between L and Ω. Also, the number of F-isomorphism is equal to $[\Omega : F]$*

A.4 Fundamental Theorem of (Finite) Galois Theory

Definition A.4.1. Let Ω/F be a field extension and $\mathrm{Aut}(\Omega/F) := \{\phi : \Omega \to \Omega | \phi_{|F} \equiv id_F\}$ be the set of F-isomorphisms. We then define:

1. For all G subgroup of $\mathrm{Aut}(\Omega/F)$

$$\Omega_G := \{\alpha \in \Omega | \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

   is a subfield called *G-invariant subfield of* Ω

2. For all M, intermediate fields between F and Ω

$$\mathrm{Aut}(\Omega/M) := \{\phi : \Omega \to \Omega | \phi \text{ is isomorphism and } \phi_{|M} \equiv id_M\}$$

   is a subgroup of $\mathrm{Aut}(\Omega/K)$

Theorem A.4.2. *Let Ω/F be an extension, then the following are equivalent:*

1. *Ω is the splitting field of a separable polynomial $f \in F[x]$*
2. *$[\Omega : F]$ is finite and $F = \Omega_{\mathrm{Aut}(\Omega/F)}$*
3. *$\exists G$ a finite subgroup of $\mathrm{Aut}(\Omega/F)$ such that $\Omega_G = F$*
4. *Ω/F is finite, normal and separable*

Definition A.4.3. Let Ω/F be a finite, normal and separable extension, then Ω it is said to be *Galois* over F and the group $\mathrm{Aut}(\Omega/F)$ is usually written as $\mathrm{Gal}(\Omega/F)$ and called *Galois group* associated to the Galois extension Ω/F.

Theorem A.4.4 (Artin)**.** *Let G be a finite subgroup of automorphisms of a field F and $E = F_G := \{\alpha \in F | \sigma(\alpha) = \alpha, \forall \sigma \in G\}$. Then F is a Galois extension of E with Galois group G, and $[F : E] = |G|$.*

The result proved by Galois in his paper was that the two defined structures in the Definition A.4.1 can be put under a bijective correspondence, hence giving an interesting structure theorem to all the Galois extension as well as their associated Galois group which is the following

Theorem A.4.5 (Fundamental Theorem)**.** *Let Ω/F be a Galois extension and let G be their Galois groups. Then for all intermediate subfield M (defining $G_M := \mathrm{Aut}(\Omega/M)$) and every subgroup H the maps:*

$$\Phi : M \mapsto G_M$$

$$\Psi : H \mapsto \Omega_H$$

are inverse maps and therefore induce a bijection between the lattices:

$$\{M | M \text{ field }, F \leq M \leq \Omega\} \leftrightarrow \{H | H \text{ subgroup of } G\}$$

Moreover,

1. *The maps Φ and Ψ are both order reversing isomorphisms, specifically,*

$$H_2 \subset H_1 \Longleftrightarrow \Omega_{H_1} \subset \Omega_{H_2}$$

2. *For all $H_1 \leq H_2, (H_2 : H_1) = [\Omega_{H_1} : \Omega_{H_2}]$ and conversely, for all $L_1 \leq L_2$(subfields), $[L_2 : L_1] = (G_{L_1} : G_{L_2})$*

3. *For every $\sigma \in G$ $\sigma H \sigma^{-1} \leftrightarrow \sigma M$*

$$\Omega_{\sigma H \sigma^{-1}} = \sigma(\Omega_H);$$

$$\sigma^{-1} G_L \sigma = G_{\sigma(L)}$$

4. *A subgroup H of G is normal if only if Ω_H/F is a normal extension, in which case:*

$$\mathrm{Gal}(\Omega_H/F) \equiv G/H$$

Proposition A.4.6. *Let E and L be extensions of F, both contained in a common field Ω. If E/F is Galois, then:*

1. *$E \wedge L/L$ is Galois*

2. *$E/E \cap L$ is Galois*

3. *The map*

$$: \mathrm{Gal}(E \wedge L/L) \longrightarrow \mathrm{Gal}(E/E \cap L)$$

$$\sigma \longmapsto \sigma_{|E}$$

is an isomorphism

Corollary A.4.7. *Let E_1 and E_2 be extensions of F contained in some common field. If both fields are Galois over F, then:*

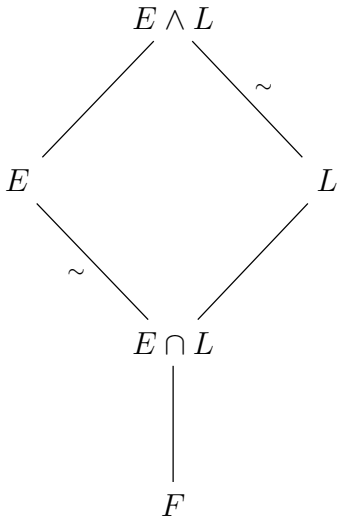
1. *$E_1 \wedge E_2$ and $E_1 \cap E_2$ are both Galois over F*
2. *the map*

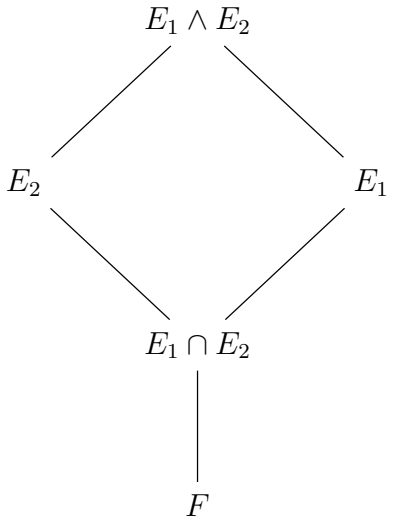
$$: \mathrm{Gal}(E_1 \wedge E_2) \longrightarrow \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$$

$$\sigma \longmapsto (\sigma_{E_1}, \sigma_{E_2})$$

is an isomorphism of $\mathrm{Gal}(E_1 \wedge E_2)$ *onto the subgroup* $H := \{(\sigma, \tau) | \sigma_{|E_1 \cap E_2} = \tau_{|E_1 \cap E_2}\}$

Following from the proposition and the corollary we give the following lattice structures for a generic Galois extension.





Appendix B

Basic Topology

In this appendix, we will list without proof the basic topological results and definitions used in the paper.

Definition B.0.1. Given a set X, a *topology* over X is a family $\tau \subset \mathcal{P}(X)$ such that:

1. $X, \emptyset \in \tau$
2. Given any $\sigma \subset \tau$, then $\bigcup_{A \in \sigma} A \in \tau$
3. For every $A, B \in \tau$, then $A \cap B \in \tau$

The elements of τ are called *open* and the pair (X, τ) is called *topological space*. Furthermore, subsets of a topological space are called *closed* if their complementary subset is open in X, and for closed sets the dual statements provided in Definition B.0.1 hold.

Example B.0.2. The easiest examples of topologies are:

- The trivial topology, where $\tau = \{X, \emptyset\}$
- The discrete topology, where $\tau = \mathcal{P}(X)$

Definition B.0.3. A *base* for a topology τ over X is a family $\mathcal{B}$ made of non-empty open sets such that $\forall A \in X, \exists \mathcal{H} \subset \mathcal{B}$ such that $A = \bigcup_{B \in \mathcal{H}} B$.

Definition B.0.4. Given $U, M \subset X$, then we say that U is a *neighbourhood* of M if there exists an open set $A \in \tau$ such that $M \subset A \subset U$.

Let's now consider a generic topological space X and a subset S.

Definition B.0.5. A point $x \in X$ is an *interior* point of S if there exists a neighbourhood U of X such that $U \subset S$. A point $x \in X$ such that for every neighbourhood U, $U \cap S \neq \emptyset$ is called *adherent*.

We can consequentially define the *interior part* $\mathring{S}$ of S as the union of all the open sets contained in S and the *closure* $\overline{S}$ as the intersection of all closed sets that contain S.

Proposition B.0.6. *S is open if and only if $S = \mathring{S}$. Similarly, S is closed if and only if $S = \overline{S}$.*

Let's now consider two topological spaces X, Y and a map $f : X \to Y$

Definition B.0.7. f is *continuous* if the inverse image $f^{-1}(U)$, for every open subset $U \subset Y$, is an open subset of X. Consequentially, the inverse image of every closed subset of Y is closed in X. In addition, When f is a continuous bijection with a continuous inverse, is called *homeomorphism*.

When given a map f between a set X and a topological space (Y, τ_Y) it is possible to induce a topology over X defined as $\tau_X = \{f^{-1}(v) | v \in \tau_Y\}$. A fundamental example of this is the *induced topology* which is associated to the map $i : X \hookrightarrow Y$, when $X \subset Y$. In this specific case, $\tau_X = \{X \cap A | A \in \tau_Y\}$.

Definition B.0.8. Let $\{X_i\}_{i \in I}$ be a family of topological spaces where I represent a generic index set, and let X be defined as the Cartesian product of the X_i. We define the *product topology* $\tau_{\mathcal{P}}$ over X as the smallest topology over X such that every canonical projection $p_i : X \to X_i$ is continuous. $(X, \tau_{\mathcal{P}})$ is then called the *topological product* of the family $\{X_i\}_{i \in I}$ (In analytic terms, this topology is the weak topology induced by the canonical projections).

Definition B.0.9. A topological space X is called *Hausdorff* if $\forall x, y \in X, x \neq y$ there exist two open sets U, V in X such that $x \in U, y \in V, U \cap V = \emptyset$.

Lemma B.0.10. *1. Every subspace of a Hausdorff space is a Hausdorff space;*

2. Every product of Hausdorff spaces is a Hausdorff space.

Definition B.0.11. Let X be a topological space

1. X is called *connected* if the only open and closed sets (clopen) are just X and the empty set;
2. Given an element $x \in X$ the *connected component* of x is the largest connected subset of X that contains x;
3. X is said to be *totally disconnected* if for every element x its connected component is the singleton $\{x\}$.

Definition B.0.12. A topological space X is said to be *compact* if every open cover of X has a finite subcover. Precisely, if $\mathcal{A}$ is a collection of open subsets of X such that $X = \bigcup_{A \in \mathcal{A}} A$ then there exists $\mathcal{B} \subset \mathcal{A}$ such that $X = \bigcup_{B \in \mathcal{B}} B$ and $\mathcal{B}$ is finite.

Lemma B.0.13. *1. Every closed subspace of a compact space is compact;*

2. Every compact subspace of a Hausdorff space is closed.

Lemma B.0.14. *Let X and Y be compact Hausdorff topological spaces and $\phi : X \to Y$ be a continuous map then ϕ is closed.*

Theorem B.0.15. *(Tychonoff's Theorem) Given a family $\{X_i\}_{i \in I}$ of compact topological spaces then their product $\prod_{i \in I} X_i$ is a compact topological space.*

Bibliography

[1] P. S. Aleksandrov and V. A. Passynkov. *Introduction into dimension theory (ru)*. Nauka, 1973, p. 574.

[2] S. Brandhorst. *Algebraische Zahlentheorie*. 2020. URL: https://www.math.uni-sb.de/ag/brandhorst/images/AZT20/AlgebraischeZahlentheorie.pdf.

[3] K. Conrad. *Infinite Galois Theory (Draft, CTNT 2020)*. 2020. URL: https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf.

[4] D. Dikranjan. *Introduction to Topological Groups*. Versione del 26.02.2018. 2018. URL: https://users.dimi.uniud.it/~dikran.dikranjan/ITG.pdf.

[5] N. Koblitz. *p-adic Numbers, p-adic Anlysis, and Zeta-Functions (Second Edition)*. Springer-Verlag, New York, 1984.

[6] J. S. Milne. *Fields and Galois Theory (v5.10)*. 2022, p. 144. URL: www.jmilne.org/math/.

[7] B. Osserman. *INVERSE LIMITS AND PROFINITE GROUPS*. 2014. URL: https://people.math.osu.edu/cogdell.1/6112-Osserman-www.pdf.

[8] J. Ruiter. *Infinite Galois Theory*. 2019. URL: https://users.math.msu.edu/users/ruiterj2/math/Documents/Notes%20and%20talks/Infinite%20Galois%20Theory.pdf.

[9] C. Williams. *MA4M3 Local Fields*. 2022. URL: https://warwick.ac.uk/fac/sci/maths/people/staff/cwilliams/lecturenotes/lecturenotes.pdf.

[10] R. Winter. *Elliptic curves over $\mathbb{Q}_p$*. 2011. URL: https://www.universiteitleiden.nl/binaries/content/assets/science/mi/scripties/bachwinter.pdf.

[11] A. Youcis. *Galois groups of local and global fields*. URL: https://alex-youcis.github.io/localglobalgalois.pdf.