Profinite Galois Groups
Grupos de Galois Profinitos

Salvador Rodríguez Sanz
Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Directores: Martínez Pérez, Concepción María
Otal Cinca, Javier
14 de Julio de 2020

Resumen

La Teoría de Galois estuvo motivada por la pregunta de si es posible expresar las soluciones de una ecuación polinómica de grado mayor o igual que cinco en términos de sus coeficientes. La respuesta fue clara: no es posible. Para ello, la propiedad de que para un polinomio con coeficientes en un cuerpo exista una fórmula función de sus coeficientes que determine sus raíces se traduce al lenguaje matemático como *resubilidad por radicales*, y para una clase particular de extensiones de cuerpos, las extensiones de Galois finitas, se establece una biyección entre los subgroups del Grupo de Galois sobre dicha extensión y sus cuerpos intermedios, de manera que existe una correspondencia unívoca entre subgrupos y subcuerpos. La caracterización de la resolubilidad por radicales lo termina de poner en manifiesto: para cada polinomio f con coeficientes en un cuerpo K, se define su Grupo de Galois como el Grupo de Galois sobre su cuerpo de escisión sobre K, de manera que f será resoluble por radicales si y solamente si el Grupo de Galois de f sea resoluble.

El presente trabajo se aleja de este enfoque para estudiar el Grupo de Galois sobre extensiones de Galois que pueden ser infinitas. Se utilizarán resultados del caso de las extensiones finitas y comprobaremos que existe, con alguna salvedad, una versión del Teorema Fundamental de la Teoría de Galois ya generalizada a extensiones de cuerpos de grado infinito. Será necesario definir una topología, la Topología de Krull, sobre dichos Grupos de Galois, y estudiar las propiedades topológicas que aparecen en ellos, así como sus consecuencias, con el fin de contar con la herramienta de la Topología para el cumplimiento del objetivo de este trabajo. Este será, a grandes rasgos, identificar una clase de grupos topológicos, los grupos profinitos, con los Grupos de Galois sobre una cierta extensión.

La memoria se encuentra dividida en tres capítulos, los cuales corresponden a dos bloques temáticos principales: la presentación de los grupos profinitos y los sistemas inversos y, posteriormente, exponer un caso concreto de estos en los Grupos de Galois sobre extensiones infinitas. Inicialmente se presentarán los grupos profinitos y los Grupos de Galois como independientes, y posteriormente, se presentarán los resultados que relacionan ambos.

En el capítulo 1, se introduce al lector en los sistemas inversos de un conjunto de espacios topológicos, así como la definición del límite inverso de un sistema inverso en términos de una propiedad universal. Esta definición se hará operativa al demostrar constructivamente que un límite inverso de un sistema inverso siempre existe, además de ser único salvo homeomorfismo. Estos límites inversos heredan una topología, y se discutirá qué invariantes topológicos heredan de los sistemas inversos. Además, se definirán los espacios profinitos como un caso particular de límite inverso de espacios finitos y discretos, y se caracterizarán tras varios resultados auxiliares en función de únicamente sus propiedades topológicas: serán espacios compactos, Hausdorff y totalmente inconexos.

En el capítulo 2, estudiaremos un caso particular de espacios profinitos: los grupos profinitos. Los sistemas inversos serán en este caso de grupos topológicos, y gracias a la previa exposición del primer capítulo, habrá una clara diferenciación entre las propiedades que aparecen como consecuencia de la estructura de espacio topológico y las nuevas caracterizaciones que se deben a la compatibilidad de la estructura algebráica de grupo con la topológica que se da en un grupo topológico.

Finalmente, se presentará un ejemplo concreto de grupos profinitos para el caso de los Grupos de Galois sobre extensiones de cuerpos que pueden ser infinitas. Primero se repasarán conceptos previos de extensiones de cuerpos y propiedades de las extensiones normales y concretamente de Galois, que son sustento de los detalles de las demostraciones de los resultados que se mencionan; definiremos un sistema inverso que nos permitirá aplicar resultados de la Teoría de Galois clásica sobre extensiones finitas y, posteriormente, demostraremos que todo Grupo de Galois sobre una extensión de Galois es isomorfo a un límite inverso de Grupos de Galois finitos y discretos, con lo que es un grupo profinito. El objetivo y colofón del trabajo será probar el resultado recíproco: todo grupo profinito será isomorfo a un Grupo de Galois sobre una extensión; tomará forma en la última sección del capítulo 3, con el teorema:

Teorema. Todo grupo profinito es isomorfo (como grupo topológico) a un Grupo de Galois sobre una extensión de cuerpos.

Prologue

The theory presented in this thesis has different purposes, depending on the chapter where it is: chapters 1 and 2 include most of the theoretical and auxiliary results that are necessary to understand the last chapter. There will be also reminders in chapter 3 of the main properties of the Galois groups of finite Galois extensions that are going to be useful for following everything in depth.

During the thesis there will be mentions to standard topological results that can be found on General Topology manuals. In our case, [8] has been the source used.

Contents

Chapter 1

Inverse Limits and Profinite Spaces

The results and concepts which are being stated in this chapter will be the knowledge basis of the further development of the thesis. The results from this part have been adapted and taken from [1].

1.1 Inverse Limits. Inverse Systems.

Definition. A set I endowed with a binary relation $\preceq$ is called a *directed partially ordered set* or briefly *directed poset* if it satisfies

(i) $i \preceq i$ for all $i \in I$;

(ii) $i \preceq j$ and $j \preceq k$ imply $i \preceq k$ for $i, j, k \in I$;

(iii) $i \preceq j$ and $j \preceq i$ imply $i = j$ for $i, j \in I$;

(iv) if $i, j \in I$ there exists some $k \in I$ such that $i, j \preceq k$.

Definition. An *inverse* or *projective system* of topological spaces over a directed poset I consists of a family $\{X_i : i \in I\}$ of topological spaces indexed by I and a collection of continuous maps $\varphi_{ij} : X_i \to X_j$ defined whenever $i \succeq j$ such that the diagrams of the form, for each $i, j, k \in I$ fulfilling $i \succeq j \succeq k$

$$\begin{tikzcd}
X_i \arrow[rr, "\varphi_{ik}"] \arrow[dr, "\varphi_{ij}"'] & & X_k \\
& X_j \arrow[ur, "\varphi_{jk}"'] &
\end{tikzcd}$$

commute, that is, $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$, assuming that $\varphi_{ii} = \mathrm{Id}_{X_i}$. From now on, we will denote such systems by $\{X_i, \varphi_{ij}, I\}$ or simply $\{X_i, \varphi_{ij}\}$ if the poset I is clear.

Remark. One can define similarly the concept of *inverse or projective system* for topological groups, as long as the sets X_i on the definition are required to be topological groups, and the maps φ_{ij}, continuous group homomorphisms. In any case, we may denote $\{X, \mathrm{Id}\}$ the trivial inverse system, consisting of $X_i = X$ for all $i \in I$ and $\varphi_{ij} = \mathrm{Id}_X$.

Definition. Let Y be a topological space, $\{X_i, \varphi_{ij}, I\}$ an inverse system of topological spaces over a directed poset I, and let $\psi_i : Y \to X_i$ be a continuous map for each $i \in I$. The family of maps $\{\psi_i\}_{i \in I}$ are said to be *compatible* if, for $i \succeq j$ the following diagram commutes

$$\begin{tikzcd}
Y \arrow[r, "\psi_i"] \arrow[d, "\psi_j"] & X_i \arrow[dl, "\varphi_{ij}"] \\
X_j &
\end{tikzcd}$$

that is, $\varphi_{ij} \circ \psi_i = \psi_j$.

Definition. Let X be a topological space together with a collection of compatible continuous maps $\{\varphi_i\}_{i\in I}$ respect to an inverse system $\{X_i, \varphi_{ij}, I\}$. We say that (X, φ_i) is an *inverse limit* or a *projective limit* of the inverse system $\{X_i, \varphi_{ij}, I\}$ if the following universal property is accomplished:

$$\begin{tikzcd} Y \arrow[r, dashed, "\psi"] \arrow[dr, "\psi_i"] & X \arrow[d, "\varphi_i"] \\ & X_i \end{tikzcd}$$

Whenever Y is a topological space and $\psi_i : Y \to X_i$, $i \in I$, is a set of compatible continuous maps, then there is a unique continuous map $\psi : Y \to X$ such that the diagram above commutes, that is, $\varphi_i \circ \psi = \psi_i$ for all $i \in I$. The maps $\varphi_i : X \to X_i$ will be called *projections*.

Given this definition, our next purpose is to make it operational and find the inverse limit of an inverse system, together with the compatible continuous maps, up to homeomorphism. This will be the aim of the next proposition.

Proposition 1.1. *Let $\{X_i, \varphi_{ij}, I\}$ be an inverse system of topological spaces over a directed poset I. Then,*

(i) There exists an inverse limit of the inverse system $\{X_i, \varphi_{ij}, I\}$;

(ii) This limit is unique in the following sense: If (X, φ_i) and (Y, ψ_i) are two limits of the inverse system $\{X_i, \varphi_{ij}, I\}$, then there is a unique homeomorphism $\varphi : X \to Y$ such that $\psi_i \circ \varphi = \varphi_i$ for each $i \in I$.

Proof. (i) Let X be the subspace of $\prod\limits_{i\in I} X_i$ given by

$$X = \left\{ (x_i) \in \prod_{i\in I} X_i \mid \varphi_{ij}(x_i) = x_j, i \succeq j \right\}$$

endowed with the subspace topology of the product topology defined in $\prod\limits_{i\in I} X_i$. Moreover, consider $\varphi_i : X \to X_i$ the restriction of the canonical projection $\pi_i : \prod\limits_{i\in I} X_i \to X_i$; the maps φ_i are continuos since they are defined in terms of the restriction of the projections π_i, which are continuous since the topology in $\prod\limits_{i\in I} X_i$ is the weak topology induced by the family $\{\pi_i\}_{i\in I}$. They are also compatible respect to $\{X_i, \varphi_{ij}, I\}$, given that $\varphi_{ij}\varphi_i((x_i)) = \varphi_{ij}(x_i) = x_j = \varphi_j((x_i))$ for $i \succeq j$. X fulfills the inverse limits universal property given above: For each topological space Y and $\psi_i : Y \to X_i$ a collection of compatible continuous maps indexed over I,

$$\begin{tikzcd} Y \arrow[r, dashed, "\psi"] \arrow[dr, "\psi_i"] & X \arrow[d, "\varphi_i"] \\ & X_i \end{tikzcd}$$

we can define $\psi(y) = (\psi_i(y))$ for each $y \in Y$. ψ is continuous since all its components are continuous, $\varphi_i\psi(y) = \varphi_i((\psi_i(y)) = \psi_i(y)$ for all $i \in I$ and this map is besides the unique one satisfying these conditions: since φ_i are restrictions of canonical projections, every map g such that $\varphi_i \circ g = \psi_i$ must satisfy that $g(y) = ((\psi_i(y))$.
(ii) Assume that (X, φ_i) and (Y, ψ_i) are both inverse limits of the inverse system $\{X_i, \varphi_{ij}, I\}$,

$$\begin{tikzcd} X \arrow[rr, dashed, bend left, "\varphi"] \arrow[dr, "\varphi_i"] & & Y \arrow[ll, dashed, bend left, "\psi"] \arrow[dl, "\psi_i"] \\ & X_i & \end{tikzcd}$$

By hypothesis, since (X,φ_i) is an inverse limit and the maps ψ_i are compatible respect to the inverse system, the universal property of (X,φ_i) shows that there exists a unique continuous map $\psi : Y \to X$ such that $\varphi_i \circ \psi = \psi_i$ for all $i \in I$. Similarly, applying the universal property of (Y,ψ_i), since the maps $\varphi_i : X \to X_i$ are compatible, there exists $\varphi : X \to Y$ such that $\psi_i \circ \varphi = \varphi_i$. Then, by composition

$$\begin{tikzcd}
X \arrow[rr, dashed, bend left, "\psi\circ\varphi"] \arrow[dr, "\varphi_i"'] & & X \arrow[ll, dashed, bend left, "\mathrm{Id}_X"] \arrow[dl, "\varphi_i"] \\
& X_i &
\end{tikzcd}$$

This diagram commutes by construction, $\varphi_i \circ \psi \circ \varphi = \psi_i \circ \varphi = \varphi_i$. According to the universal property in 1.1 concerning the definition of the inverse limit (X,φ_i), they both have to coincide, $\psi \circ \varphi = \mathrm{Id}_X$. Analogously $\varphi \circ \psi = \mathrm{Id}_Y$, and φ is a bijection. Since its inverse is ψ, which is also continuous, φ is a homeomorphism with the same properties as the statement of the proposition. □

Remark. Let $\{X_i,\varphi_{ij},I\}$ an inverse system, by 1.1, there always exists an inverse limit of the inverse system, considered with the canonical projections φ_i from the proof of 1.1. The inverse limit will be denoted by $\varprojlim_{i\in I} X_i$ or simply $\varprojlim X_i$, if the poset I is clear.

1.1.1 Topological Properties of Inverse Limits

Proposition 1.2. *Let $\{X_i,\varphi_{ij},I\}$ be an inverse system of topological spaces over a directed poset I.*

(i) If each X_i is Hausdorff, so is $\varprojlim X_i$;

(ii) If each X_i is totally disconnected, so is $\varprojlim X_i$.

Proof. From now on, and without further notice, we will consider without loss of generality the inverse limit found on 1.1. All the inverse limits are homeomorphic by 1.1, so it suffices to study the topological properties on a concrete inverse limit, as they are invariant under homeomorphism.

(i) If all the spaces X_i are Hausdorff, then the product set (with the product topology) $\prod\limits_{i\in I} X_i$ is Hausdorff, and since $\varprojlim X_i$ is a subspace of the product, it is also Hausdorff since this property is hereditary on products and subspaces.
(ii) The product of totally disconnected spaces is analogously totally disconnected, and this property is hereditary on subspaces. Thus, $\varprojlim X_i$ is totally disconnected. □

Lemma 1.3. *If $\{X_i,\varphi_{ij},I\}$ is an inverse system of Hausdorff topological spaces, then $\varprojlim_{i\in I} X_i$ is a closed subspace of $\prod\limits_{i\in I} X_i$.*

Proof. Equivalently, we have to prove that $\prod_{i\in I} X_i - \varprojlim X_i$ is open. Let $(x_i) \in \prod_{i\in I} X_i - \varprojlim X_i$, there exists $r \succeq s$ such that $\varphi_{rs}(x_r) \neq x_s$. Since all the spaces X_i are Hausdorff, there are two open disjoint neighbourhoods U and V of $\varphi_{rs}(x_r)$ and x_s respectively. Moreover, since the map φ_{rs} is continuous, and $\varphi_{rs}(x_r) \in U$, by continuity there is an open neighbourhood U' of x_r such that $\varphi_{rs}(U') \subseteq U$, so considering the basic open subset $W = \prod_{i\in I} V_i$ where $V_r = U'$, $V_s = V$ and $V_i = X_i$, for $i \neq r,s$, $(x_i) \in W \subseteq \prod_{i\in I} X_i - \varprojlim X_i$ and $\varprojlim X_i$ is closed. □

Proposition 1.4. *Let $\{X_i,\varphi_{ij},I\}$ be an inverse system of compact Hausdorff topological spaces over the directed poset I. Then, $\varprojlim\limits_{i\in I} X_i$ is a compact Hausdorff topological space.*

Proof. By Tychonoff Theorem, $\prod_{i\in I} X_i$ is compact since all the spaces X_i are compact. The product of Hausdorff spaces is also Hausdorff, and then $\prod_{i\in I} X_i$ is Hausdorff. As $\varprojlim_{i\in I} X_i$ is a subspace of $\prod_{i\in I} X_i$, it is Hausdorff, and by 1.3, it is closed and subspace of a compact space, so compact, and $\varprojlim_{i\in I} X_i$ is compact Hausdorff as the claim states. □

Proposition 1.5. *Let $\{X_i, \varphi_{ij}, I\}$ be an inverse system of compact Hausdorff nonempty topological spaces X_i over the directed set I. Then, $\varprojlim X_i$ is nonempty.*

Proof. For each $j \in I$ let

$$Y_j = \left\{ (x_i) \in \prod_{i\in I} X_i \mid \varphi_{jk}(x_j) = x_k,\ k \preceq j \right\}$$

All the spaces X_i are nonempty by hypothesis, by the Axiom of Choice $\prod_{i\in I} X_i \neq \emptyset$ and there is an element $(x_i) \in \prod_{i\in I} X_i$. There is a sequence (y_i) where $y_r = \begin{cases} \varphi_{jr}(x_j) & \text{if} \quad r \preceq j \\ x_r & \text{if} \quad r \npreceq j \end{cases}$ For every $k \preceq j$, since $j \preceq j$ and $\varphi_{jj} = \mathrm{Id}_{X_j}$, $\varphi_{jk}(y_j) = \varphi_{jk}(\varphi_{jj}(x_j)) = \varphi_{jk}(x_j) = y_k$ so $(y_i) \in Y_j$. In particular, $Y_j \neq \emptyset$. With an analogous argument as in 1.3, Y_j is closed for each $j \in I$ and if $j \preceq j'$ by definition $Y_{j'} \subseteq Y_j$ and therefore given that I is a poset, the family of sets $\{Y_j \mid j \in I\}$ has the finite intersection property, i.e., any finite collection of sets belonging to this family has nonempty intersection; since all the sets Y_j are closed and subspaces of $\prod_{i\in I} X_i$, which is compact due to Tychonoff Theorem, the intersection $\bigcap_{j\in I} Y_j$ has to be nonempty. Also,

$$\varprojlim X_i = \bigcap_{j\in I} Y_j \neq \emptyset$$

so $\varprojlim_{i\in I} X_i$ is nonempty. □

Proposition 1.6. *Let (X, φ_i) be an inverse limit of an inverse system $\{X_i, \varphi_{ij}, I\}$ of non-empty compact Hausdorff spaces indexed by I. The following assertions hold:*

(i) $\varphi_i(X) = \bigcap_{j\succeq i} \varphi_{ji}(X_j)$;

(ii) The family $\mathscr{F} = \{\varphi_i^{-1}(U) \mid i \in I, U \text{ open in } X_i\}$ forms a base of neighborhoods for the topology on X;

(iii) If Y is a subset of X satisfying $\varphi_i(Y) = X_i$ for each $i \in I$, then Y is dense in X;

(iv) A map $\theta : Y \to X$ is continuous if and only if each map $\varphi_i \circ \theta$ is continuous;

(v) If $f : X \to A$ is a continuous map from X to a discrete space, then f factors through X_i for some i: for some $i \in I$ there is a continuous map $g : X_i \to A$ such that $f = g \circ \varphi_i$.

Proof. (i): Consider $j \succeq i$; by the compatibility of the maps $\{\varphi_i\}_{i\in I}$ respect to the inverse system $\{X_i, \varphi_{ij}, I\}$, $\varphi_{ji} \circ \varphi_j = \varphi_i$, $\varphi_i(X) = \varphi_{ji} \circ \varphi_j(X) \subseteq \varphi_{ji}(X_j)$ for all $j \succeq i$, therefore $\varphi_i(X) \subseteq \bigcap_{j\succeq i} \varphi_{ji}(X_j)$.

Now, let $i \in I$ be fixed and $a \in \bigcap_{j\succeq i} \varphi_{ji}(X_j)$; for $j \succeq i$ we define

$$Y_j = \{ y \in X_j \mid \varphi_{ji}(y) = a \}$$

By hypothesis all the spaces X_i are Hausdorff, so $\{a\}$ is closed. φ_{ji} continuous, $Y_j = \varphi_{ji}^{-1}(a)$ is closed for all $j \succeq i$ and subspaces of compact spaces, so compact. For all $j \succeq i$, $Y_j \neq \emptyset$ and for each k that $i \preceq j \preceq k$ and $y_k \in Y_k$, by definition $a = \varphi_{ki}(y_k) = \varphi_{ji} \circ \varphi_{kj}(y_k)$ and $\varphi_{kj}(y_k) \in Y_j$, so we can define an inverse system $\{Y_j, \psi_{kj}, j \succeq i\}$ where the maps ψ_{kj} are the restrictions of φ_{kj} for $k \succeq j \succeq i$ to the spaces Y_l both in the start space and the target space. By 1.5, $\varprojlim_{j\succeq i} Y_j \neq \emptyset$ and there exists $(b_j)_{j\succeq i} \in \varprojlim_{j\succeq i} Y_j$; For every $k \succeq j \succeq i$, $\varphi_{kj}(b_k) = b_j$ and $\varphi_{ji}(b_j) = b_i = a$. The next step which shall be followed is to extend the sequence $(b_j)_{j\succeq i}$; in order to do that, if $l \in I$ and $l \nsucceq i$, for $j \succeq i, l$ one defines $b_l = \varphi_{jl}(b_j)$; this choice is independent of j: For any other choice of $j' \succeq i, l$ and $k \succeq j, j'$

$$\varphi_{jl}(b_j) = \varphi_{jl} \circ \varphi_{kj}(b_k) = \varphi_{kl}(b_k) = \varphi_{j'l} \circ \varphi_{kj'}(b_k) = \varphi_{j'l}(b_{j'})$$

Thus, $(b_i)_{i\in I}$ belongs to $\varprojlim_I Y_i \subseteq X$ and $\varphi_i(b) = b_i = a$ since its a restriction of the canonical projection.

(ii):X is endowed with the subspace topology of the product, all the open sets in X have the form $P = X \cap \prod_{i\in I} U_i$ where $U_i = X_i$ for all $i \in I\backslash\{i_1,\dots i_m\}$, and U_{i_r} open in X_{i_r} for all $r = 1,\dots,m$. Therefore, $\mathscr{F}$ will be a basis of the topology in X if for every $a \in P$ there is U open in X_k such that $a \in \varphi_k^{-1}(U) \subseteq P$. Let $a = (a_i) \in P$ and $k \in I$ so that $k \succeq i_1,\dots i_m$. The sets $\varphi_{ki_r}^{-1}(U_{i_r})$ are open since φ_{ki_r} is continuous, $a_k \in \varphi_{ki_r}^{-1}(U_{i_r})$ since $\varphi_{ki_r}(a_k) = a_{i_r} \in U_{i_r}$; Let $U = \bigcap_{r=1}^{m} \varphi_{ki_r}^{-1}(U_{i_r})$, by finite intersection of open sets, U is open and it is a neighbourhood of a because $\varphi_k(a) = a_k \in \varphi_{ki_r}^{-1}(U_{i_r})$ and for every $b = (b_i) \in \varphi_k^{-1}(U)$, $\varphi_k(b) = b_k \in U$ and $b_{i_r} = \varphi_{ki_r}(b_k) \in U_{i_r}$, so $a \in \varphi_k^{-1}(U) \subseteq P$ as we wanted to see.

(iii): For every nonempty open set in X_i, namely U, $U = X_i \cap U = \varphi_i(Y) \cap U \neq \emptyset$, so $\varphi_i(Y) \cap U \neq \emptyset$ which implies $Y \cap \varphi_i^{-1}(U) \neq \emptyset$. Since $\mathscr{F}$ is a basis by (ii), Y is dense in X.

(iv) from (ii): If θ is continuous, by composition so is $\varphi_i \circ \theta$. On the opposite direction, since $\mathscr{F}$ is a basis for the topology in X, it suffices to show that $\theta^{-1}(\varphi_i^{-1}(U))$ is open for every open set U, but $\theta^{-1}(\varphi_i^{-1}(U)) = (\varphi_i \circ \theta)^{-1}(U)$ and $\varphi_i \circ \theta$ is continuous.

(v): Let $A_0 = f(X)$. A_0 is compact because f is continuous and X is compact. Also, A_0 is discrete since it is a subspace of A. Thus, A_0 is finite.[1] Let $a \in A_0$, define $Y_a = f^{-1}(a)$; since A is discrete, $\{a\}$ is open and by continuity Y_a is open. Because of the same reason, $\{a\}$ is closed in A and by the continuity of f, Y_a is closed. By 1.4 X is compact, Y_a is a closed subset of X and hence Y_a is compact so it can be expressed as a finite union of basis elements from $\mathscr{F}$ in (ii). Owing to the fact that A_0 is finite and $\mathscr{F}$ from (ii) is a basis, each Y_a is open so it is a union of elements in $\mathscr{F}$, and by compactness there is a finite family $\varphi_{j_1}^{-1}(U_1),\dots,\varphi_{j_n}^{-1}(U_n)$ such that each Y_a is a union of some of those open sets. Then, for $k \in I$ satisfying $j_1,\dots,j_n \preceq k$ the compatibility of the maps φ_l yields to $\varphi_{kj_r} \circ \varphi_k = \varphi_{j_r}$, $\varphi_{j_r}^{-1}(U_r) = \varphi_k^{-1}(\varphi_{kj_r}^{-1}(U_r))$ and for each $a \in A_0$, $Y_a = \varphi_k^{-1}(V_a)$ where V_a is an open set of X_k. Let $D = X_k \backslash \cup_{a\in A_0} V_a$, notice $f^{-1}(A_0) = X = \varphi_k^{-1}(\cup_{a\in A_0} V_a)$ and $D \cap \varphi_k(X) = \emptyset$, so from (i) $D \cap \bigcap_{j\succeq k} \varphi_{jk}(X_j) = \emptyset$; each set $\varphi_{lk}(X_l)$ is closed since they are compact subspaces of a Hausdorff space, D is closed and a subspace of a compact set, so it is compact and the family $\{D \cap \varphi_{jk}(X_j)\}_{j\succeq k}$ can not have the finite intersection property since it has empty intersection; there must be $l_1,\dots,l_s$ indices such that $D \cap \varphi_{l_1k}(X_{l_1}) \cap \cdots \cap \varphi_{l_sk}(X_{l_s}) = \emptyset$. Picking $i \succeq l_1,\dots l_s$, for $k \preceq l \preceq i$ by commutativity of the inverse system diagrams in 1.1, $\varphi_{ik}(X_i) = \varphi_{lk}(\varphi_{il}(X_i)) \subseteq \varphi_{lk}(X_l)$ and

$$\varphi_{ik}(X_i) \subseteq \varphi_{l_1k}(X_{l_1}) \cap \cdots \cap \varphi_{l_sk}(X_{l_s}) \Rightarrow D \cap \varphi_{ik}(X_i) = \emptyset \Leftrightarrow \varphi_{ik}(X_i) \subseteq \bigcup_{a\in A_0} V_a \tag{1.1}$$

Finally, let $W_a = \varphi_{ik}^{-1}(V_a)$ for each $a \in A_0$, W_a is open, $W_{a_1} \cap W_{a_2} = \emptyset$ if $a_1 \neq a_2$: We constructed the sets V_a so that they are union of the sets $\varphi_{kj_r}^{-1}(U_r)$; since $\varphi_{j_r}^{-1}(U_r) \neq \emptyset$, $\varphi_{kj_r}^{-1}(U_r) \subseteq \varphi_k(X)$ and each V_a is contained in $\varphi_k(X)$. Then, for every $x \in W_{a_1} \cap W_{a_2}$, $\varphi_{ik}(x) \in V_{a_1} \cap V_{a_2}$, but we assumed that $a_1 \neq a_2$, $\emptyset = Y_{a_1} \cap Y_{a_2} = \varphi_k^{-1}(V_{a_1} \cap V_{a_2})$ so $V_{a_1} \cap V_{a_2} \subseteq X_k \backslash \varphi_k(X)$, $V_{a_1} \cap V_{a_2} = \emptyset$ and $W_{a_1} \cap W_{a_2} = \emptyset$. By (1.1) for every $x \in X_i$ there is an $a \in A_0$ such that $\varphi_{ik}(x) \in V_a$, so $x \in \varphi_{ik}^{-1}(V_a) = W_a$, $X_i = \cup_{a\in A_0} W_a$ and the map $g : X_i \to A$ mapping W_a to $a \in A$ is continuous as A is discrete and the sets W_a are open, and $f = g \circ \varphi_i$ by construction. □

[1] A space X is *limit point compact* or *weakly countably compact* if every infinite subset of X has at least one accumulation point, i.e., for all $B \subseteq X$ s.t. $|B| \geq \aleph_0$, $B' \neq \emptyset$. Every compact set is limit point compact, so A_0 is limit point compact, but this set is also discrete, so it must not have any infinite subset, so to speak, it is finite.

Lemma 1.7. *Let $\{X_i, \varphi_{ij}, I\}$ be an inverse system of compact Hausdorff spaces and X a compact Hausdorff space. Suppose that $\{\varphi_i\}_{i\in I}$ is a set of compatible continuous and surjective maps. Thus, the corresponding induced map $\theta : X \longrightarrow \varprojlim X_i$ given by $x \mapsto (\varphi_i(x))$ is surjective.*

Proof. Considering the constant inverse system $\{X, \mathrm{Id}, I\}$, the maps $\{\varphi_i\}_{i\in I}$ from X to X_i are compatible on $\{X_i, \varphi_{ij}, I\}$, for every $i \succeq j$, $\varphi_{ij} \circ \varphi_i = \varphi_j$. Let $(x_i) \in \varprojlim X_i$, and $\tilde{X}_i = \varphi_i^{-1}(x_i) \neq \emptyset$ by surjectivity. X_i is Hausdorff for all $i \in I$, then $\{x_i\}$ is closed in X_i, and by continuity, $\tilde{X}_i$ is a closed subset of X compact, so $\tilde{X}_i$ is compact for all $i \in I$. For each $x \in \tilde{X}_i$, $\varphi_i(x) = x_i$ and if $i \succeq j$, $\varphi_j(x) = \varphi_{ij}(x_i) = x_j$, we have that $x \in \tilde{X}_j$ and $\tilde{X}_i \subseteq \tilde{X}_j$. Every finite intersection of the sets $\tilde{X}_i$ is non-empty: for every family $i_1, \dots, i_r \in I$ there exists $j \succeq i_1, \dots, i_r$ and $\tilde{X}_j \subseteq \tilde{X}_{i_1} \cap \cdots \cap \tilde{X}_{i_r}$. X is compact, so applying the finite intersection property

$$\bigcap_{i\in I} \tilde{X}_i \neq \emptyset$$

and $x \in \bigcap_{i\in I} \tilde{X}_i$ satisfies $\theta(x) = (x_i)$. □

1.2 Profinite Spaces

After all these propositions, the next step is to characterize a certain class of topological spaces which will give the reader the chance to understand why all the last results have been shown. This is nevertheless the last section in which some properties of topological spaces will be discussed. Again, the main source for this section has been [1].

Definition. A topological space X which arises as the inverse limit

$$X = \varprojlim_{i\in I} X_i$$

of finite spaces X_i endowed with the discrete topology is called *Profinite Space* or *Boolean Space*.

Lemma 1.8. *Let X be a compact Hausdorff topological space, and let $x \in X$. Then, the connected component C of x is the intersection of all closed and open neighbourhoods of x.*

Proof. Let $\{U_t \mid t \in T\}$ be the family of all open and closed neighbourhoods of x, and

$$A = \bigcap_{t\in T} U_t$$

Every closed and open neighbourhood U of x contains C: indeed, $C = C \cap X = C \cap (U \cup U^c) = (C \cap U) \cup (C \cap U^c)$. U is closed and open, so as C is connected it has to be either $C \cap U = \emptyset$ or $C \cap U^c = \emptyset$. Recall that $C \cap U \neq \emptyset$ as $x \in C \cap U$; it has to be $C \cap U^c = \emptyset$ and $C \subseteq U$, for every closed and open neighbourhood of x, hence $C \subseteq A$. It remains to show that $A \subseteq C$, but by the maximality of C, it suffices to see that A is connected. Let U, V be two closed sets in A (and in X, as A is closed) such that $A = U \cup V, U \cap V = \emptyset$, we are going to prove that either U or V are empty. Moreover, U, V are closed subspaces of X, which is compact, so U and V are compact and disjoint. X is Hausdorff by hypothesis, so there are two U', V' open sets such that $U \subseteq U', V \subseteq V'$ and $U' \cap V' = \emptyset$. Moreover,

$$[X \backslash U' \cup V'] \cap A = \emptyset \Rightarrow X \backslash U' \cup V' \subseteq \bigcup_{t\in T} U_t^c$$

$X \backslash U' \cup V'$ is a closed subspace of X, which is compact, so $X \backslash U' \cup V'$ is compact and there is a finite set $F \subseteq T$ satisfying

$$X \backslash U' \cup V' \subseteq \bigcup_{t\in F} U_t^c \Rightarrow [X \backslash U' \cup V'] \cap \bigcap_{t\in F} U_t = \emptyset \tag{1.2}$$

where $B = \bigcap_{t\in F} U_t$ is an open and closed neighbourhood of x. On the other hand, by (1.2) $B \subseteq U' \cup V'$ and $B = B \cap (U' \cup V') = (B \cap U') \cup (B \cap V')$, $x \in B$. Without loss of generality, if $x \in B \cap U'$, $B \cap U'$ is open and closed and a neighbourhood of x, so by definition $A \subseteq B \cap U' \subseteq U'$ and it has to be $V = V \cap A \subseteq V' \cap A = \emptyset$. □

Definition. An equivalence relation R on a topological space X is said to be *open* (or respectively, *closed*) if for every $x \in X$, the equivalence class xR is an open set in X.

Remark. Take into account the following properties regarding the definition above:

(a) If R is open, then it is also closed, since X is the union of disjoint open sets (the equivalence classes) and each class xR is the complementary of a union of open sets.

(b) R can be considered as the subset of $X \times X$ given by $R = \{(x,y) \in X \times X \mid x \sim y\}$. In such case, the concepts of being open as an equivalence relation or being open as a subspace of $X \times X$ are equivalent: If R is open, then if $(x,y) \in R$, $x \sim y$ and $xR \times yR$ is an open set (by product) contained in R, so R is an open subset of $X \times X$. Conversely, if $R \subseteq X \times X$ is open, $(x,x) \in R$ by reflexivity and there exists a neighbourhood U such that $(x,x) \in U \times U \subseteq R$ and $x \in U \subseteq xR$.

This concept of open equivalence relations will be necessary here to prove the following characterization of profinite spaces.

Proposition 1.9. *Let X be a topological space. Then, the following assertions are equivalent:*

(i) X is a profinite space;

(ii) X is compact Hausdorff and totally disconnected;

(iii) X is compact Hausdorff and admits a basis of closed and open sets for its topology.

Proof. $(i) \Rightarrow (ii)$: Let X be a profinite space, say $X = \varprojlim_I X_i$ where the spaces X_i are finite and discrete, by 1.2 since each X_i is Hausdorff and totally disconnected, so is X; Every X_i is compact since they are finite and discrete, by 1.4, X is also compact, and the result follows.

$(ii) \Rightarrow (iii)$: Let X be a compact Hausdorff and totally disconnected space. Let W be an open neighborhood of a point $x \in X$. It suffices to show that there is a closed and open neighborhood U of x such that $x \in U \subseteq W$. Let $\{U_t \mid t \in T\}$ be the family of all closed and open neighborhoods of x. The connected component of x is $\{x\}$ as X is totally disconnected, by 1.8

$$\{x\} = \bigcap_{t \in T} U_t$$

W is open, $X \backslash W$ is closed and subset of X. $X \backslash W$ is therefore compact and disjoint from $\bigcap_{t \in T} U_t$ and by the same argument as in the proof of 1.8 there is $F \subseteq T$ finite such that

$$(X \backslash W) \cap \left(\bigcap_{t \in F} U_t \right) = \emptyset \tag{1.3}$$

and $x \in \bigcap_{t \in F} U_t \subseteq W$.

$(iii) \Rightarrow (i)$: Let X compact Hausdorff such that it admits a basis of closed and open sets for its topology. Denote by $\mathscr{R}$ the collection of all open equivalence relations R on X, and let $\psi_R : X \to X/R$ be the family of projections into the quotient space X/R for each $R \in \mathscr{R}$; for such $R \in \mathscr{R}$, $X = \bigsqcup_{x \in X} xR$; since each equivalence class xR is open, and by compactness, there are $x_1R, \ldots, x_nR$ equivalence classes such that $X = \bigsqcup_{i=1}^{n} x_iR$ and every equivalence class of X/R equals some of the x_iR, so $X/R = \{x_1R, \ldots, x_nR\}$. X/R is finite and discrete since its topology is the collection of sets $\{U \subseteq X/R \mid \psi_R^{-1}(U) \text{ is open in } X\}$, as every union of open sets and in particular of open equivalence classes is open. What's more, the set $\mathscr{R}$ is ordered as follows: if $R, R' \in \mathscr{R}$, then $R \succeq R' \Leftrightarrow xR \subseteq xR'$ for all $x \in X$, and $\mathscr{R}$ is a partially ordered set; it is also directed, for every $R_1, R_2 \in \mathscr{R}$, defining $R_1 \cap R_2$ the equivalence relation with classes $xR_1 \cap xR_2$, $R_1 \cap R_2 \succeq R_1, R_2$. Now, if $R \succeq R'$, let $\psi_{RR'} : X/R \to X/R'$ given by $\psi_{RR'}(xR) = xR'$. $\{X/R, \psi_{RR'}, \mathscr{R}\}$ is an inverse system over $\mathscr{R}$ and it remains to see that $X \cong \varprojlim_{R \in \mathscr{R}} X/R$. For that purpose, remember

$$\psi_R : X \longrightarrow X/R$$

is a surjection (since its the projection of X into the quotient) and continuous (by the topology defined on X/R) for all $R \in \mathscr{R}$, so the induced map

$$\begin{aligned} \psi\colon X &\longrightarrow \varprojlim_{R\in\mathscr{R}} X/R \\ x &\mapsto (\psi_R(x))_{R\in\mathscr{R}} \end{aligned}$$

is continuous (given that so are its components) and surjective by 1.7. In order to prove then that ψ is a homeomorphism, providing that X is compact, it is only left to see that ψ is injective: let $x, y \in X$, $x \neq y$. By hypothesis, since X is Hausdorff and it admits a basis of closed and open neighborhoods, there is an open and closed set U such that $x \in U$, $y \notin U$ and $U, X\backslash U$ are both open. Let $R \in \mathscr{R}$ (and $\mathscr{R}$ is not empty) be the relation defined in X by

$$x \sim y \Leftrightarrow x, y \in U$$

It is obviously reflexive, symmetric and transitive, so R becomes an equivalence relation which is also open by definition. Take into account that X/R has two elements, these are $U, X\backslash U$ and $\psi_R(x) \neq \psi_R(y)$ so $\psi(x) \neq \psi(y)$ they can not be equal. □

1.2.1 Further Comments

The main purpose of this chapter has been studying some properties of the inverse systems and inverse limits that are going to be necessary for the following development of the thesis. However, and not less important, in the upcoming sections the reader will acknowledge that we are going to focus on a particular case of these inverse systems, not over the category of topological spaces, but over the one of topological groups. Since these topological groups own a topological structure compatible with the algebraic one, the object of this chapter was not other than discerning which properties come only from the topological structure; In any case, we could have defined the inverse systems and limits over the category of topological groups, always assuming that the morphisms are, in such case, continuous homomorphisms, and the operations on the product sets $\prod_{i\in I} G_i$ are carried out componentwise.

Chapter 2

Profinite Groups

Along the previous chapter it has been shown how certain topological spaces which come up as inverse limits of discrete and finite topological spaces may be characterized in terms of its topological properties. Beginning with an inverse system $\{X_i, \varphi_{ij}, I\}$, one builds the inverse limit in terms of the continuous maps φ_{ij} and the restrictions of the canonical projections. Here, we will discuss the properties that appear when we restrict our inverse systems to be formed by topological groups. The main source has been [1].

2.1 Topological Groups. Definitions and Properties.

Definition. A *topological group* G is a set with two structures:

(i) $(G,\cdot)$ is a group with the product $\cdot : G\times G \to G$;

(ii) (G,τ) is a topological space.

which have a compatibility within the two of them, understanding it as the maps

$$\begin{aligned} \eta\colon G\times G &\to G & \nu\colon G &\to G \\ (g,h) &\mapsto g\cdot h & g &\mapsto g^{-1} \end{aligned}$$

are both continuous. From now on, we will denote $UV = \eta(U\times V) = \{u\cdot v \mid u\in U, v\in V\}$ and $U^{-1} = \nu(U) = \{u^{-1} \mid u \in U\}$ for $U,V \subseteq G$.

Remark. As a result of the compatibility, we can deduce consequences regarding the topological structure of G:

(i) Let $a\in G$ fixed, the *translations*

$$\begin{aligned} L_a\colon G &\to G & \text{and } R_a\colon G &\to G \\ g &\mapsto ag & g &\mapsto ga \end{aligned}$$

are both continuous since they are both restrictions of η and also bijective. Since $L_a^{-1} = L_{a^{-1}}$, $R_a^{-1} = R_{a^{-1}}$, they are homeomorphisms and every local basis $\mathscr{B}(x)$ for $x\in G$ is fully determined by the local basis of neighborhoods in 1_G, $\mathscr{B}(1_G)$.

(ii) G is **Hausdorff** if and only if $\{1_G\}$ is closed (and therefore, all the sets $\{a\} = L_a(1)$, $a\in G$ are closed): The implication $\Rightarrow)$ is clear, G is Hausdorff and therefore a T_1-space, so $\{1\}$ is closed. For $a,b\in G$ such that $a\neq b$, $G\backslash\{a^{-1}b\}$ is an open neighbourhood of 1, $1 = \eta(1,1^{-1}) = \eta(1,\nu(1))$ and by the continuity of η and ν there are two open neighbourhoods U,V of 1 such that $UV^{-1} \subseteq G\backslash\{a^{-1}b\}$. $aU = L_a(U)$, $bV = L_b(V)$ are open neighbourhoods of a,b respectively and they are disjoint: if $c\in aU\cap bV$, $c = au, u\in U$ and $c = bv, v\in V$ so $au = bv$ and $a^{-1}b = uv^{-1} \in UV^{-1}$, contradiction.

(iii) If $H \leq G$, then H is a topological group with the subspace topology of G, and η, ν are continuous by restriction. If $K \trianglelefteq G$, the space G/K is a topological group with the quotient topology, that is, the weak topology induced by the projection $\pi : G \to G/K$; i.e., $\tau_{G/K} = \{U \subseteq G/K \mid \pi^{-1}(U) \in \tau_G\}$. Moeover, π is open: for every open set U in G, $\pi^{-1}\pi(U) = UK$. Given that for every $k \in K$, $Uk = R_k(U)$ is open as so is U, $UK = \bigcup_{k \in K} Uk$ is open by union of open sets.

(iv) For a normal subgroup $K \trianglelefteq G$, G/K is Hausdorff if and only if K is closed in G: If G/K is Hausdorff, for $x \in G \backslash K$, it follows that $xK \neq K$ and there are two open sets U, V in G/K such that $xK \in U, K \in V$. Thus, $\pi^{-1}(U)$ is an open neighbourhood of x and $x \in \pi^{-1}(U) \subseteq G \backslash K$. Conversely, for two coclasses $xK \neq yK$, equivalently $xy^{-1} \notin K$ and as η and ν are both continuous and $xy^{-1} = \eta(x, \nu(y))$, there are two neighbourhoods V of x and W of y such that $xy^{-1} \in VW^{-1} \subseteq G \backslash K$ and $\pi(V), \pi(W)$ are two disjoint open sets that separate xK and yK: bear in mind that if there exist $v \in V$ and $w \in W$ that $vK = wK$, $vw^{-1} \in K$ which is a contradiction with $VW^{-1} \subseteq G \backslash K$.

2.2 Profinite Groups

Definition. A topological group G is *profinite* if it is the inverse limit of an inverse system formed by finite groups G_i endowed with the discrete topology. More precisely, there exists an inverse system $\{G_i, \varphi_{ij}, I\}$ of finite and discrete topological groups such that

$$G = \varprojlim_{i \in I} G_i$$

Example. Let G be a group and let $\mathscr{N}$ be the family

$$\mathscr{N} = \{N \trianglelefteq G \mid G/N \text{ is finite and discrete}\}$$

$\mathscr{N}$ is nonempty since $G \in \mathscr{N}$, and $\mathscr{N}$ is a directed poset by defining the order $M \preceq N$ if and only if $N \leq M$, i.e., N is subgroup of M. If $M, N \in \mathscr{N}$ and $N \succeq M$ let the epimorphism $\varphi_{NM} \colon G/N \to G/M$ which maps $xN \mapsto xM$ and is well defined because $N \leq M$. $\{G/N, \varphi_{NM}, N \in \mathscr{N}\}$ is an inverse system and the profinite group $\hat{G} := \varprojlim_{N \in \mathscr{N}} G/N$ is called the *profinite completion* of G.

For example, consider $G = (\mathbb{Z}, +)$. G is abelian, every subgroup $H \leq G$ is normal, and $H = n\mathbb{Z}$ where $n \in H$ is the integer in H with the lowest modulus $|n|$. Each group $\mathbb{Z}/n\mathbb{Z}$ is finite and endowed with the discrete topology. The profinite completion of G is $\hat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ and, as a set, it is formally the set of sequences $a = (a_1, a_2, \ldots)$ such that $a_n \equiv a_m (\operatorname{mod} m)$ when $m|n$.

Lemma 2.1. *Let $G = \varprojlim_{i \in I} G_i$ where $\{G_i, \varphi_{ij}, I\}$ is an inverse system of finite and discrete groups G_i and let $\varphi_i : G \to G_i$, $i \in I$, be the restriction of the canonical projections as in 1.1. Then, $\{S_i \mid S_i = \ker \varphi_i\}$ is a fundamental system of open neighborhoods of the identity element 1 in G.*

Proof. Let V be an open neighborhood of 1 in G. G inherits the topology as a subspace of $\prod_{i \in I} G_i$, and $V = W \cap G \subseteq G \subseteq \prod_{i \in I} G_i$ for some W open set in $\prod_{i \in I} X_i$. Given that each G_i is discrete, $\{1_{G_i}\}$ is open for every G_i, $1_G = (1_{G_i})_{i \in I}$ and there is a finite number of indices in I, namely $i_1, \ldots, i_t$ that

$$1 \in \left(\prod_{i \neq i_1, \ldots, i_t} G_i \right) \times \{1\}_{i_1} \times \cdots \times \{1\}_{i_t} \subseteq W \subseteq \prod_{i \in I} G_i$$

Let i_0 such that $i_0 \succeq i_1, \ldots i_t$. We have that

$$\underbrace{G \cap \left[\left(\prod_{i \neq i_0} G_i \right) \times \{1\}_{i_0} \right]}_{N} = \underbrace{G \cap \left[\left(\prod_{i \neq i_1, \ldots, i_t} G_i \right) \times \{1\}_{i_1} \times \cdots \times \{1\}_{i_t} \right]}_{M}$$

Since $i_0 \succeq i_1, \ldots, i_t$, if $g = (g_i) \in N$, $g_{i_j} = \varphi_{i_0 i_j}(1_{i_0}) = 1_{i_j}$, $N \subseteq M$. Looking into the reverse containment, $x \in M$ implies that $x_{i_0} = \varphi_{i_0}(x) \in \ker \varphi_{i_0 i_1} \cap \cdots \cap \ker \varphi_{i_0 i_t}$ and by the compatibility of the maps $\{\varphi_i\}_{i \in I}$ as stated in 1.1, $\varphi_{i_0 i_t} \circ \varphi_{i_0} = \varphi_{i_t}$ and $1 = \varphi_{i_t}(x) = x_{i_t}$. Finally, it is clear that

$$1_G \in N = S_{i_0} = G \cap \left[\left(\prod_{i \neq i_0} G_i \right) \times \{1\}_{i_0} \right] \subseteq V$$

Hence, for every neighborhood V of 1_G in G there exists some $i \in I$ such that $S_i \subseteq V$ and $\{\ker \varphi_i\}_{i \in I}$ is a fundamental system of neighborhoods for $1 \in G$, or in other words, a local basis.

□

Lemma 2.2. *In a compact topological group G, a subgroup H is open if and only if H is closed of finite index.*

Proof. Without loss of generality, we will assume that the index is over left cosets, even though the number of left cosets or right cosets of H in G is the same.
H is open, $G = \bigsqcup_{x \in G} xH$. For every $x \in G$ the co-classes are open as so is H and $xH = L_x(H)$. The set $\{xH\}_{x \in G}$ is an open covering of G, there is a finite number of open coclasses $x_1H, \ldots, x_nH$ such that $G = \bigsqcup_{i=1}^n x_iH$ and $|G : H| = |\{x_1H, \ldots, x_nH\}|$ is finite, so H has finite index. Every x_iH is also closed: $x_iH \cap x_jH = \emptyset$ for every $i \neq j$ and $G \backslash x_iH = \bigsqcup_{j \neq i, 1 \leq j \leq n} x_iH$ is a finite union of open sets, so it is open. Every x_iH is closed, and $H = L_{x_i^{-1}}(x_iH)$ is closed. Similarly, if H is closed and has finite index, there are finitely many left coclasses of H in G, and $G = \bigsqcup_{i=1}^n x_iH$. H is closed, so is x_iH, and they are all disjoint. By a similar argument than before, x_iH is open since $G \backslash x_iH$ is a union of closed sets, so it is closed, and H is open. □

Theorem 2.3. *The following assertions on a topological group G are equivalent:*

(i) G is a profinite group;

(ii) G is a compact Hausdorff totally disconnected space, and for each open normal subgroup U of G, G/U is discrete and finite.

(iii) G is compact and the identity element $1 \in G$ *admits a fundamental system* $\mathscr{U}$ *of open neighborhoods U such that* $\bigcap_{U \in \mathscr{U}} U = 1$*, and each U is an open normal subgroup of G with G/U finite and discrete.*

(iv) The identity element 1 *of G admits a fundamental system* $\mathscr{U}$ *of open neighborhoods U such that each U is a normal subgroup of G with G/U finite and discrete and*

$$G = \varprojlim_{U \in \mathscr{U}} G/U.$$

Proof. $(i) \Rightarrow (ii)$: Let G be profinite, say

$$G = \varprojlim_{i \in I} G_i$$

where G_i are finite and discrete groups. As a topological space, G is a profinite space and G is compact, Hausdorff and totally disconnected by 1.9. Let $U \trianglelefteq G$ be open, since $1 \in U$, by 2.1, the set $\{S_i\}$ is a fundamental system of open neighborhoods of the identity element $1 \in G$ and there exists $i \in I$ such that $1 \in S_i \leq U$. In addition, $S_i = \text{Ker } \varphi_i$ and it is the kernel of a homomorphism, so it is a normal subgroup of G, $S_i \trianglelefteq G$. By the isomorphism theorem, $G/S_i \cong \text{Im } \varphi_i \leq G_i$; S_i is open, so by 2.2, S_i is closed and has finite index. It follows that the isomorphism between finite groups $G/S_i \cong \text{Im } \varphi_i$ is a homeomorphism: G is compact and $G/S_i = \pi(G)$ is compact as it is the image of the continuous map $\pi : G \rightarrow G/S_i$, the isomorphism is continuous as Ker φ_i is open. Then, G/S_i is discrete. Applying the third isomorphism theorem, $G/U \cong (G/S_i)/(U/S_i)$, finite and discrete by isomorphism.
$(ii) \Rightarrow (iii)$: Since G is compact Hausdorff and totally disconnected, it admits a basis of closed and

open sets for its topology by 1.9, (iii). Let $\mathscr{V}$ the family of closed and open neighborhoods of 1. The intersection $\bigcap_{V\in\mathscr{V}} V$ equals the connected component of 1 in G by 1.8, which is $\{1\}$, so

$$\bigcap_{V\in\mathscr{V}} V = 1$$

It suffices to show that $V \in \mathscr{V}$ contains an open normal subgroup U of G, and G/U will be finite and discrete by hypothesis. Let $F = (G\backslash V) \cap V^2$. Since V is closed and G is compact, V is compact, and by continuity, so is V^2; hence, since G is compact and Hausdorff, V^2 is closed and F is closed. Let $x \in V$; then, $x \in G\backslash F$ and since $G\backslash F$ is open, and η is continuous, there are V_x, S_x neighborhoods of x and 1 respectively such that $V_x, S_x \subseteq V$ and $V_x S_x \subseteq G\backslash F$. Additionally, $V \subseteq \bigcup_{x\in V} V_x$ and by compactness $V \subseteq \bigcup_{i=1}^n V_{x_i}$. Denote $S = \bigcap_{i=1}^n S_{x_i}$, $W = S \cap S^{-1}$. W is symmetric, i.e., $W^{-1} = W$, and an open neighborhood of 1 (by intersection, as ν, the inversion, is a homeomorphism since its inverse is itself and it maps open sets to open sets); $W \subseteq V$ and $VW \subseteq G\backslash F$, or equivalently $VW \cap F = \emptyset$. Additionally, $VW \subseteq V^2$, $VW \subseteq V$ so by induction over $n \in \mathbb{N}$, $VW^n \subseteq V$. Furthermore,

$$R := \bigcup_{n\in\mathbb{N}} W^n$$

is open by union of open sets and a subgroup of G. Therefore, R is closed and of finite index, and the *core* of R

$$R_G = \bigcap_{x\in G} x^{-1}Rx$$

is closed and a normal subgroup of G, so it has finite index, and R_G is open. R_G is the open normal subgroup and neighborhood of 1 we were looking for:

$$R_G \leq R \subseteq VR \subseteq \bigcup_{n\in\mathbb{N}} VW^n \subseteq V$$

$(iii) \Rightarrow (iv)$: by hypothesis, G admits a fundamental system of open neighborhoods $\mathscr{U}$ of 1 such that $\bigcap_{U\in\mathscr{U}} U = 1$ and each $U \in \mathscr{U}$ is an open normal subgroup of G where G/U is finite and discrete. Similarly as in previous results, $\mathscr{U}$ can be easily defined as a directed poset by defining $U \succeq V \Leftrightarrow U \leq V$ for $U, V \in \mathscr{U}$. Considering the inverse system $\{G/U, \varphi_{UV}, \mathscr{U}\}$ where $\varphi_{UV} : G/U \to G/V$ is the natural epimorphism for $U \succeq V$, and the maps φ_U are the canonical projections into the quotient G/U, they induce a continuous homomorphism

$$\psi : G \to \varprojlim_{U\in\mathscr{U}} G/U$$

which maps $x \in G \mapsto (\varphi_U(x))_{U\in\mathscr{U}}$. Since the projections are all surjective and $\{1\}$ is closed by intersection of closed sets (as the sets $U \in \mathscr{U}$ are open in G compact, and we apply 2.2), then G is Hausdorff, and ψ is onto by 1.7. G is compact so it is enough to show that ψ is injective: if $x \in G$ and $\psi(x) = 1$, then $x \in U$ for all $U \in \mathscr{U}$, so $x = 1$. As ψ is a continuous bijection with starting space a group G compact, ψ is a homeomorphism of topological groups and $G \cong \varprojlim_{U\in\mathscr{U}} G/U$.
$(iv) \Rightarrow (i)$: By definition the implication holds. □

Chapter 3

Infinite Galois Extensions. Krull Theorem.

This final chapter will introduce an extension of the fundamental theorem of Galois Theory to infinite Galois extensions. The answer will be given by Wolfgang Krull's theorem of inclusion-reversing bijections. Before that, we will focus on some concepts and prepositions. Most of the results from the Krull topology on the Galois groups have been taken from [2], [4] and [8]. For the results concerning field extensions, the principal reference has been [3].

3.1 Field Extensions

We are beginning this part with some key words from Field Theory which will be of importance in the following results.

Definitions. Let E and K be two fields:

(i) E is a *field extension* of K if K is a subfield of E. In this dissertation, field extensions are denoted as E/K. In particular, we will call *degree of the extension* the dimension of E as a K-vector space, denoted as $[E:K] := \dim_K E$. The extension will be *finite* if the degree is finite, or *infinite* otherwise.

(ii) If X is a subset of E and E/K is a field extension, we will denote the *subring* $K[X] \subseteq E$ as the set of **finite** K-linear combinations of finite products of powers of elements in X. More concretely, if $a \in K[X]$, there exist $\alpha_1, \ldots, \alpha_r$ such that $a = f(\alpha_1, \ldots, \alpha_r)$ for $f \in K[x_1, \ldots, x_r]$. Also, $K(X) \subseteq E$ is the set of all elements $ab^{-1} \in E$ where $b \neq 0$ and $a, b \in K[X] \subseteq E$; Therefore, $K(X)$ is isomorphic to the field of fractions of $K[X]$, and it is a *subfield* of E.

(iii) An element $\alpha \in E$ is *algebraic over* K if there exists a nonzero polynomial $p \in K[x]$ such that $p(\alpha) = 0$. The extension E/K is *algebraic* if every element in E is algebraic over K. Oppositely, $\alpha \in E$ is *transcendental* if there is no polynomial $p \in K[x]$ which has α as a root, and E/K is *transcendental* if there is some element in E that is transcendental.

(iv) If E/K is a field extension, then E is *finitely generated* if $E = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$. A finitely generated extension E/K will be simple if $E = K(\alpha)$ for some $\alpha \in E$, which will be a *primitive element* of E.

(v) K is *algebraically closed* if the only algebraic extension of K is K itself.

Proposition 3.1. *Let $K \subseteq E \subseteq F$. Then, $[F:K] = [F:E][E:K]$. In particular, if E/K and F/E are finite, so is F/K.*

Proof. The result follows by considering a particular basis $\{\alpha_i\}_{i\in I}$ of F as an E-vector space and $\{\beta_j\}_{j\in J}$ a basis of E as a K-vector space. Let $\alpha \in F$, $\alpha = \sum_{i\in I} r_i\alpha_i$ where $r_i \in E$ for all $i \in I$. Analogously, $r_i = \sum_{j\in J} s_{ij}\beta_j$ for some $s_{ij} \in K$ for every $j \in J$. Thus,

$$\alpha = \sum_{j\in J}\sum_{i\in I} s_{ij}\beta_j\alpha_i$$

The family $\mathscr{F} = \{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ generates F over K because every element of F is a K-linear combination of elements in $\mathscr{F}$. The elements in $\mathscr{F}$ are linearly independent over K: for $\{t_{ij}\}_{(i,j)\in I\times J}$ such that

$$\sum_{(i,j)\times I\times J} t_{ij}\alpha_i\beta_j = \sum_{i\in I}\sum_{j\in J} t_{ij}\alpha_i\beta_j = \sum_{i\in I}\left(\sum_{j\in J} t_{ij}\beta_j\right)\alpha_i$$

As the family $\{\alpha_i\}$ is linearly independent over $K \subseteq E$,, $\sum_{j\in J} t_{ij}\beta_j = 0$ for every $i \in I, j \in J$. On the same way, by the linear independence of $\{\beta_j\}$ over K, $t_{ij} = 0$ for every $i \in I, j \in J$. In particular, $[F:K] = |I\times J| = |I||J| = [F:E][E:K]$. □

Remark. (i) Following the same notation as before, for every set $X \subseteq E$, $K(X)$ is a field and, certainly, it is the smallest field that contains X and E: for any other field F such that $K \subseteq F$ and $X \subseteq F$, let $a \in K[X]$ and $b \in K[X], b \neq 0$ then $ab^{-1} \in F$ and $K(X) \subseteq F$. Like in the $K[X]$ case, if $u \in K(X)$, $u = ab^{-1}$ for $a,b \in K[X]$, $b \neq 0$ and there exist $x_1,\dots,x_k \in X$ such that $a \in K[x_1,\dots,x_k]$ and $y_1,\dots,y_r \in X$ that $b \in K[y_1,\dots,y_r]$. Then, $a,b \in K[x_1,\dots,x_k,y_1,\dots,y_r]$ and $u \in K(x_1,\dots,x_k,y_1,\dots,y_r)$.

(ii) A finite extension E/K is algebraic: for evey $\alpha \in E$, if the degree of the extension is $n = [E:K] < \infty$, then $1,\alpha,\dots,\alpha^n$ is linearly dependent and there exist $t_0,\dots,t_n \in K$ such that $t_0 + t_1\alpha + \dots + t_n\alpha^n = 0$, so α is a root of the polynomial $p = t_0 + t_1x + \dots + t_nx^n$, and $p(\alpha) = 0$.

Proposition 3.2. *Let E/K be a field extension and $\alpha \in E$.*

(i) If $\alpha \in E$ is algebraic over K, there is a unique monic irreducible polynomial $q \in K[x]$ that $q(\alpha) = 0$ and $K(\alpha) \cong K[\alpha], [K(\alpha):K] = deg(q)$ and $1,\alpha,\dots,\alpha^{n-1}$ is a basis of $K(\alpha)$ over K, where $n = \deg(q)$.

(ii) If α is transcendental, then $[K(\alpha):K]$ is necessarily infinite, and there is an isomorphism $K(\alpha) \cong K(x)$ that fixes K elementwise, where $K(x)$ is the field of fractions of the polynomial ring $K[x]$.

Proof. Consider $\psi : K[x] \to K(\alpha)$ be the evaluation homomorphism given by $p \mapsto p(\alpha)$ for every $p \in K[x]$. ψ is a ring homomorphism. Remember that $K[\alpha] = \{t_0 + t_1\alpha + \dots + t_n\alpha^n \mid n \in \mathbb{N},\ t_i \in K\ \}$, and $\operatorname{Im}\psi = \{f(\alpha) \mid f \in K[x]\} = K[\alpha]$.
(ii): If $\alpha \in E$ is trascendental, there is no polynomial with coefficients in K such that α is a root of p, so $\operatorname{Ker}\psi = 0$ and by the isomorphism theorem $K[X] \cong K[\alpha]$ and both rings are isomorphic. Thus, the fields of fractions are isomorphic, $K(\alpha) \cong K(x)$, and the extension $K(\alpha)/K$ is necessarily infinite: by the previous remark, if it would be finite, then it would be algebraic, which is a contradiction.
(i): If $\alpha \in E$ is algebraic, there exists a nonzero polynomial $p \in K[x]$ such that $p(\alpha) = 0$ so $\psi(p) = 0$, $\operatorname{Ker}\psi \neq 0$. $\operatorname{Ker}\psi$ is an ideal of $K[x]$ and $K[x]$ is an euclidean domain, every ideal is principal, so there exists a unique monic polynomial $q \in K[x]$ such that $\operatorname{Ker}\psi = (q)$. Also, q is irreducible: as K is a field, if $q = gh$ then $g(\alpha) = 0$ or $h(\alpha) = 0$ and either $g \in \operatorname{Ker}\psi$ or $h \in \operatorname{Ker}\psi$, but they both have lower degree than q, which is a contradiction. The ideal (q) is maximal as q is irreducible, so $K[x]/(q) \cong K[\alpha]$ and $K[\alpha]$ is a field, $K[\alpha]$ contains all the inverses of the linear combinations of powers of α, so $K[\alpha] = K(\alpha)$. Finally, notice that $1,\alpha,\dots,\alpha^{n-1}$ is a basis of $K(\alpha)$: if $t_0 + t_1\alpha + \dots + t_{n-1}\alpha^{n-1} = 0$, then the polynomial $r(x) = t_0 + t_1x + \dots + t_{n-1}x^{n-1}$ belongs to $\operatorname{Ker}\psi$ and has lower degree than q, contradiction, $t_0 = \dots = t_{n-1} = 0$. In addition, let a polynomial $f \in K[x]$, by the division algorithm there exist

$c, r \in K[x]$ where $\deg(r) < \deg(q) = n$ and $f = qc + r$, $f(\alpha) = r(\alpha)$ where r has at most degree $n-1$, and $f(\alpha)$ is a linear combination in K of the family $1, \alpha, \dots, \alpha^{n-1}$. Given that if $\alpha \in E$ is algebraic $K(\alpha) = \{f(\alpha) \mid f \in K[x]\}$, $1, \alpha, \dots, \alpha^{n-1}$ spans $K(\alpha)$ over K. □

Definition. Let E/K be a field extension and $\alpha \in E$ be algebraic over K. The monic irreducible polynomial $q \in K[x]$ from 3.2 is called *minimal polynomial* or *irreducible polynomial* of α.

Corollary 3.3. *Let E/K be a field extension, $\alpha_1, \dots, \alpha_r \in E$ algebraic over K. Then, $K(\alpha_1, \dots, \alpha_r)/K$ is finite.*

Proof. As $\alpha_1 \in E$ is algebraic over K, applying 3.2, $K(\alpha_1)/K$ is finite. Inductively, α_2 is algebraic over K and $K[x] \subseteq K(\alpha_1)[x]$, so α_2 is algebraic over $K(\alpha_1)$ and the extension $K(\alpha_1, \alpha_2)/K(\alpha_1)$ is finite, so consequently $K(\alpha_1, \alpha_2)/K$ is finite by 3.1. Reasoning in the same way for every α_i, the claim follows. □

The fact of K being algebraically closed has important consequences or different characterizations, closer to the aim of the definition. If K is algebraically closed, then the only algebraic extension of K is trivially K. Let p be irreducible and monic in $K[x]$, then, the ideal (p) of $K[x]$ is maximal, $F = K[x]/(p)$ is a field, and p has degree at least 1. F/K is a field extension, doing the identification $K = \{t + (p) \mid t \in K\}$. The element $x + (p) \in F$ is a root of $p \in K[x] \subseteq F[x]$ and $F \cong K(x + (p))$. The extension F/K is finite by 3.2, so algebraic. K is algebraically closed, $F \cong K$, and p must have degree 1, so every irreducible polynomial over K has degree 1. Assuming that in $K[x]$ all the irreducibles have degree 1 yields to K being algebraically closed, since for every algebraic extension E/K and $\alpha \in E$, there is a monic irreducible polynomial $p \in K[x]$ such that $p(\alpha) = 0$, but p must have degree 1, and $p = x - \alpha \in K[x]$, $\alpha \in K$. Another way of stating something equivalent is defining K to be a field in which every non-constant polynomial in $K[x]$ has a root in K; for every algebraic extension E/K, the minimal polynomial of $\alpha \in E$ has a root in K, but it is irreducible, so it must have degree one and since it is monic it is of the form $x - \alpha \in K[x]$, $\alpha \in K$. If all the irreducibles have degree 1, as $K[x]$ is a unique factorization domain, then every non-constant polynomial splits in linear factors and they have at least one root in K.

3.1.1 The Algebraic Closure

Preliminarily, we mention an important extension property for homomorphism into algebraically closed fields. After defining the algebraic closure, it will become fully useful to extend homomorphisms to algebraic extensions.

Theorem 3.4. *Every homomorphism of a field K into an algebraically closed field can be extended to every algebraic extension of K.*

Proof Reference. The proof shows the existence of the extension using Zorn's Lemma. For further details, see [3], IV.§4, 4.2.

□

Theorem 3.5. *Every field K has an algebraic extension that contains a root of every nonconstant polynomial with coefficients in K. Consequently, every field K has an algebraic extension $\bar{K}$ that is algebraically closed, and $\bar{K}$ is unique up to isomorphism that fixes K elementwise.*

Proof Reference. The proof can be found split in two results on [3], IV. §4,4.3. and [3], IV. §4, 4.4. □

As a result, 3.5 yields to the definition:

Definition. An algebraic closure of a field K is a field extension $\bar{K}/K$ that is algebraically closed. It always exists by 3.5, and it is unique up to isomorphism, so we will refer to $\bar{K}$ as *the algebraic closure* of K.

Remark. Theoretically, the fact that for every field K there is an algebraic extension, namely $\bar{K}$, such that it is algebraically closed, has a direct consequence when studying the factorization of polynomials in $K[x]$: by the first part of 3.5, for every $p \in K[x]$, there exists an extension K_1/K that contains a root of p, $a_1 \in K_1$, and $x - a_1 \in K_1[x]$, $p = (x - a_1)q$ where $q \in K_1[x]$. Inductively, there exists K_2/K_1 and therefore extension of K such that q has a root in K_2 and eventually there would be an extension K_n/K such that all the roots of p are in K_n. Since every algebraic extension E/K is contained in $\bar{K}$, there is always a field extension of K in which p has all its roots, which is $\bar{K}$, for every $p \in K[x]$.

3.1.2 Normal and Galois Extensions

Definition. Let K be a field. A polynomial $f \in K[x]$ is called *separable* if it has no multiple roots in some algebraic closure of K. For an algebraic extension E/K, an element $\alpha \in E$ is *separable* over K if its minimal polynomial is separable; furthermore, the extension itself E/K is called *separable* if all its elements are separable over K.

Definitions. Let K be a field.

(i) A polynomial $f \in K[x]$ splits in a field extension E/K when it has a factorization $f = a(x - \alpha_1)\dots(x - \alpha_r) \in E[x]$. A splitting field over K of a polynomial $f \in K[x]$ is a field extension E/K such that f splits in E and E is generated over K by the roots of f. In other words, the splitting field of f over K is the smallest field that contains K and the roots of f, which are always in $\bar{K}$.

(ii) An extension E/K such that $K \subseteq E \subseteq \bar{K}$ is *normal* if E is the splitting field over K of a set of polynomials.

Definition. A field extension E/K is called *Galois Extension* if it is normal and separable. Without further notice, we will say briefly that E is *Galois* over K.

When K has characteristic 0, every irreducible polynomial $f \in K[x]$ has degree ≥ 1 and its derivate is always non-zero, $f' \neq 0$. f has a multiple root α if and only if $f(\alpha) = f'(\alpha) = 0$ and particularly $x - \alpha | f, x - \alpha | f'$. However, if $f \in K[x]$ is irreducible in K, f does not divide f' as f' has lower degree than f, so $\mathrm{mcd}(f, f') = 1$ and f can't have multiple roots: by Bézout's Identity, there exist $p, q \in K[x]$ satisfying $pf + qf' = 1$ and if f has a multiple root α, $1 = pf(\alpha) + qf'(\alpha) = 0$, contradiction. A field extension E/K when the characteristic of K is 0 is always separable and it will be Galois if and only if it is normal.

Example. For example, in $\mathbb{Q}$, the extension $\mathbb{Q}(i)/\mathbb{Q}$ is normal since it is the splitting field of $x^2 + 1 \in \mathbb{Q}[x]$ and as it is normal and $\mathrm{car}(\mathbb{Q}) = 0$, $\mathbb{Q}(i)/\mathbb{Q}$ is Galois.
When F has characteristic 0, $H = \{\text{roots of } x^n - 1\}$ is a cyclic group of order n with the product of $\bar{F}$, and there exists χ such that H is generated by χ, $H = \langle \chi \rangle$. χ is called an *n-primitive root of unity*. The field $F(\chi)$ contains H and $F(\chi) = F(1, \chi, \dots, \chi^{n-1})$, $F(\chi)/F$ is normal and separable since $\mathrm{car}(F) = 0$, so a Galois extension.

Proposition 3.6. *Let E/K be a finite separable extension. Then, E/K is simple.*

Proof. The proof can be followed with complete details in [3] or [6] for the general cases, and in [7] when K is infinite. □

Proposition 3.7. *Let E/K be a normal extension, then E/K is algebraic.*

Proof. Let $F = \{\alpha \in E \mid \alpha \text{ is algebraic over } K\}$, K is a subfield of F as every element $t \in K$ is a root of $x - t \in K[x]$; we claim that F is subfield of E: for every $a, b \in F$, there exist two polynomials $p, q \in K[x]$ such that $p(a) = 0$ and $p(b) = 0$, and the extensions $[K(a) : K]$ and $[K(b) : K]$ are both finite by 3.2. Then, $[K(a)(b) : K] = [K(a)(b) : K(a)][K(a) : K]$, $K(a, b)/K$ is finite by 3.3 , so it is algebraic. Notice that $a - b, ab^{-1} \in K(a, b)$, they are roots of some polynomials, and $a - b, ab^{-1} \in F$, so F is a subfield of E. By definition $F \subseteq E$, and since E/K is normal, E is generated by K and roots of some polynomials with coefficients in K, algebraic elements belonging to F, $E \subseteq F$, so $F = E$ and E is algebraic. □

Corollary 3.8. *Let E/K be a Galois extension. For every $\alpha \in E$, the extension $K(\alpha)/K$ is finite.*

Proof. E/K being Galois implies that E/K is normal, so E/K is algebraic by 3.7. The claim then follows by 3.2. □

Proposition 3.9. *Let K be a field and E/K an algebraic extension. The extension E/K is normal if and only if every irreducible polynomial $p \in K[x]$ with a root in E splits in E.*

Proof. Let E/K be a normal extension of K. By 3.7, E/K is an algebraic extension of K, so in this case the assumption of E/K algebraic is redundant. Let $p \in K[x]$ be an irreducible polynomial with a root $\beta \in E$, assume that p is monic; then, p is by uniqueness the minimal polynomial of β, and by 3.5 and 3.1.1, in the extension $\bar{K}/K$, p splits and $\bar{K}$ contains all the roots of p. Let $\gamma \in \bar{K}$ be another root, the minimal polynomial of γ is also p and there is a field isomorphism $\varphi : K(\beta) \to K(\gamma) \subseteq \bar{K}$ such that $\varphi(\beta) = \gamma$ and φ fixes K elementwise. By 3.4, since $E/K(\beta)$ is algebraic as so is E/K, there exists $\psi : E \to \bar{K}$ homomorphism of fields that extends φ; As E/K is normal and ψ preserves K, for every polynomial $q \in K[x]$, and a a root of q, $\psi(a)$ is another root of q, as $q(\psi(a)) = \psi(q(a)) = \psi(0) = 0$. Consequently, $\psi(E) \subseteq E$. Also, $\beta \in K(\beta) \subseteq E$, so $\psi(\beta) = \gamma \in E$. Hence, E contains all the roots of p, and p splits in E.

For the other implication, as E/K is algebraic, for every $\alpha \in E$ the irreducible polynomial p_α of α is well-defined by 3.2 and it splits in E by hypothesis, $E = K(\{\text{roots of } p_\alpha \mid \alpha \in E\})$ resulting in E/K normal. □

Corollary 3.10. *Let E/K be an algebraic extension. Then, E/K is a normal extension if and only if $\varphi(E) \subseteq E$ for every $\varphi : E \to \bar{K}$, where φ is a homomorphism that fixes K elementwise.*

Proof. By an analogous argument like in 3.9 for ψ, we have $\varphi(E) \subseteq E$ in the first implication, as φ fixes K element by element and E is the splitting field of a set of polynomials, so it permutes the roots of the polynomials with coefficients in K. Conversely, for every irreducible polynomial $p_\alpha \in K[x]$ with a root $\alpha \in E$, without loss of generality we can assume that p_α is monic. Then, p_α is the irreducible polynomial of α over K. If p has degree 1, $\alpha \in K$, so assume that $\alpha \notin K$. As p_α has at least degree 2, there exists another root η of p_α in $\bar{K}$ and there is an isomorphism $\rho : K(\alpha) \to K(\eta)$ that maps α to η and fixes K. This morphism can be extended by 3.4 to φ, and $\varphi(\alpha) = \eta \in E$. By 3.9, E/K is normal. □

Corollary 3.11. *Let E/K be a normal extension and $K \subseteq M_1, M_2 \subseteq E$ subfields. If $\sigma : M_1 \to M_2$ is an isomorphism that fixes K elementwise, then there exists an isomorphism $\theta : E \to E$ that extends σ.*

Proof. By 3.7, E/K is algebraic. M_1 is a between field of E/K, so E/M_1 is algebraic, and as E/K is algebraic, E is contained in $\bar{K}$ which is algebraically closed as we discussed, so by 3.4, there exists $\theta : E \to \bar{K}$ a field homomorphism that extends σ. θ is a monomorphism as it is a field homomorphism, and as E/K is normal, there is a set $\mathscr{S}$ of polynomials such that $E = K(X_f \mid f \in \mathscr{S})$ where X_f is the set of roots of $f \in \mathscr{S}$, contained in $\bar{K}$. As σ fixes K element by element, θ fixes every polynomial in $K[x]$ and for every $a \in X_f$, $f(\theta(a)) = \theta(f(a))$, so $\theta(X_f) \subseteq X_f$. Since θ is injective and each X_f is finite, it has to be $\theta(X_f) = X_f$ for every $f \in \mathscr{S}$. It follows that $\theta(E) = E$, and θ is an automorphism of E that fixes K. □

3.1.3 The Galois Group. The Main Theorem for Finite Extensions.

Definitions. Let $\mathrm{Aut}(E)$ be the group of automorphisms of a field E.

(i) Let E/K be an extension. The *Galois Group* of the extension E/K is the group

$$\mathrm{Gal}(E/K) = \{\sigma : E \to E \in \mathrm{Aut}(E) \mid \sigma(k) = k \, \forall k \in K\} \leq \mathrm{Aut}(E)$$

(ii) For every field F and $G \leq \mathrm{Aut}(F)$, the *fixed field* of G is $F^G := \{\alpha \in F \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$.

Example. (i): Let p be prime and F be the finite field of p^n elements; F is an extension of $\mathbb{Z}_p$ as it is a finite field and F is the splitting field of the polynomial $x^{p^n} - x \in \mathbb{Z}_p[x]$, up to isomorphism. Therefore, the extension $F/\mathbb{Z}_p$ is normal, and as a $\mathbb{Z}_p$-vector space, F is linearly isomorphic to $[F : \mathbb{Z}_p]$ copies of $\mathbb{Z}_p$, and $|F| = p^n$, so $[F : \mathbb{Z}_p] = n$. The polynomial $f = x^{p^n} - x$ has at most p^n roots and every element in F is a root of f; moreover, $f' = p^n x^{p^n-1} - 1 = -1$, $\mathrm{mcd}(f', f) = \mathrm{mcd}(-1, f) = 0$ and the roots of f are all different, so $F = \{\text{roots of } f\}$. Particularly, if $x \in F^* = F \backslash \{0\}$ then $x^{p^n-1} = 1$ and F^* is the set of $p^n - 1$-roots of the unity, and F^* is cyclic as an abelian group with the product. Thus, there exists $\chi \in F$ such that $F = \mathbb{Z}_p(\chi)$, $\chi \in F^*$. Let $\alpha \in \mathrm{Aut}(F)$ such that $\alpha(x) = x^p$. By Fermat's Little Theorem, since p is prime, $x^{p-1} = 1$ for every $x \in \mathbb{Z}_p$. Also, α is a field homomorphism and it fixes $\mathbb{Z}_p$, so $\alpha \in \mathrm{Gal}(F/\mathbb{Z}_p)$. Furthermore, α must have order n: if it has order $r < n$, then for all $x \in F$ we have $\alpha^r = \mathrm{Id}_F$ so $x^{p^r} = x$ and F would have p^r elements. Then, $\langle \alpha \rangle \leq \mathrm{Gal}(F/\mathbb{Z}_p)$. Finally, notice that χ is algebraic over $\mathbb{Z}_p$ and we can take p its irreducible polynomial, which divides f, so is separable since the roots of f are all different, its roots are in F. Thus, p splits in F and it has $\deg(p) = [\mathbb{Z}_p(\chi) : \mathbb{Z}_p] = [F : \mathbb{Z}_p] = n$ roots. There are at most n automorphisms of F such that they fix $\mathbb{Z}_p$: for every $\tau \in \mathrm{Gal}(F/\mathbb{Z}_p)$, τ fixes p and it is fully determined by $\tau(\chi)$, which has to be another root of p, so $|\mathrm{Gal}(F/\mathbb{Z}_p)| \leq n$ and $\langle \alpha \rangle = \mathrm{Gal}(F/\mathbb{Z}_p)$. $\mathrm{Gal}(F/\mathbb{Z}_p)$ is cyclic of order n, α is called the *Fröbenius automorphism.*
(ii): Following the same notation as 3.1.2, $F(\chi)/F$ is Galois since $F(\chi)$ is the splitting field of the polynomial $x^n - 1$ over F, and separable as F has characteristic 0. Every automorphism $\beta \in \mathrm{Gal}(F(\chi)/F)$ is fully determined by $\beta(\chi)$. Furthermore, $x^n - 1 \in F[x]$ and $\chi^n = 1$, $\beta(\chi)^n = \beta(\chi^n) = 1$ and $\beta(\chi) \in \langle \chi \rangle$, say $\beta(\chi) = \chi^i$. For any other automorphism $\iota \in \mathrm{Gal}(F(\chi)/F)$, $\iota(\chi) = \chi^j$ and $\iota\beta(\chi) = \beta\iota(\chi)$, so $\iota\beta = \beta\iota$ and they commute, $\mathrm{Gal}(F(\chi)/F)$ is abelian.

Proposition 3.12. *Let E/K be a not necessarily Galois extension and L an intermediate field such that $K \subseteq L \subseteq E$. Then, if L/K is normal, $\sigma(L) = L$ for all $\sigma \in Gal(E/K)$.*

Proof. As L/K is normal, there is a set $\mathscr{S}$ of polynomials in $K[x]$ such that L is the splitting field of every $p \in \mathscr{S}$ over K. For every $f \in \mathscr{S}$ with set of roots X_f, $X_f \subseteq E \subseteq \bar{K}$ is finite and every $\sigma \in \mathrm{Gal}(E/K)$ fixes f, $\sigma(f) = f$. For every $a \in X_f$, $\sigma(a) \in X_f$ as $f(\sigma(a)) = \sigma(f(a)) = 0$. Thus, $\sigma(X_f) \subseteq X_f$ and as X_f is finite and σ is injective, $\sigma(X_f) = X_f$ as in 3.11. Then the result is straightforward, $\sigma(L) = \sigma(K(X_f \mid f \in \mathscr{S})) = K(X_f \mid f \in \mathscr{S}) = L$ for every $\sigma \in \mathrm{Gal}(E/K)$. □

Proposition 3.13. *Let E/K be Galois. Then, $|Gal(E/K)| = [E : K]$ and $E^{Gal(E/K)} = K$.*

Proof. The proof of $|\mathrm{Gal}(E/K)| = [E : K]$ will not be discussed here, see [3] V.§3, 3.6 or [6] §4, 4.3. Let us see that $E^{\mathrm{Gal}(E/K)} = K$. Every automorphism in $\mathrm{Gal}(E/K)$ fixes K, so for every $t \in K$, $\sigma(t) = t$ for all $\sigma \in \mathrm{Gal}(E/K)$, $K \leq E^{\mathrm{Gal}(E/K)}$. Now, let $\alpha \in E^{\mathrm{Gal}(E/K)}$, assume that $\alpha \notin K$. E/K is normal, by 3.7 E/K is algebraic and there is a monic irreducible polynomial with coefficients in K, namely p, such that $p(\alpha) = 0$ by 3.2. As $\alpha \notin K$, p has at least degree 2, and there is another root $\beta \in \bar{K}$ ofp_α in the algebraic closure of K. E/K is Galois over K, so in particular is separable, and $\beta \neq \alpha$. Indeed, E/K is normal, by 3.9, $\beta \in E$ and there is a field isomorphism $\rho : K(\alpha) \to K(\beta) \subseteq \bar{K}$ such that it fixes K elementwise and maps $\rho(\alpha) = \beta$. E/K is particularly normal, by 3.11, there exists $\theta : E \to E$ an isomorphism that extends ρ and fixes K elementwise since so does ρ. Thus, $\theta \in \mathrm{Gal}(E/K)$, and $\theta(\alpha) = \beta \neq \alpha$, contradiction. □

Lemma 3.14. *Let E/K be algebraic and separable. If the minimal polynomial over K of each $\alpha \in E$ has degree at most n, then E/K is finite over K and $[E : K] \leq n$.*

Proof. Let $\alpha \in E$,p_α the minimal polynomial of α. The subset $\{\deg(p_\alpha) \mid \alpha \in E\} \subset \mathbb{N}$ is bounded by n, there exists $x \in E$ such that $\deg p_x$ is maximal: that is, the only $\gamma \in E$ such that $\deg(p_\gamma) \geq \deg(p_x)$ is $\gamma = x$. For any other $\beta \in E$, the extension $K(\beta, x)/K$ is separable since so is E/K, and it is finite by 3.3, as x, β are algebraic over K since E/K is algebraic. Applying 3.6 there exists $\gamma \in E$ such that $K(x, \beta) = K(\gamma)$. By hypothesis, $\deg(p_\gamma) \leq n$ and $\deg(p_\gamma) = [K(\gamma) : K] \leq n$. Furthermore, $K(x) \leq K(\gamma)$ and $[K(x) : K] = \deg(p_x) \geq \deg(p_\gamma) = [K(\gamma) : K]$ thus $K(x) = K(\gamma)$, and every $\beta \in E$ belongs to $K(x)$, $E = K(x)$ and $[E : K] = [K(x) : K] \leq n$. □

Proposition 3.15. *If G is a finite group of automorphisms of a field E, then E is a finite Galois extension of E^G and, moreover, $Gal(E/E^G) = G$.*

Proof. Let $F = E^G$ and $\alpha \in E$. The set $\{\sigma(\alpha) \mid \sigma \in G\}$ is finite since so is G, and has cardinality $\leq |G|$. Denote more conviniently $\{\alpha_1, \ldots, \alpha_k\} = \{\sigma(\alpha) \mid \sigma \in G\}$ where $\alpha_1 = \alpha$ since $\mathrm{Id}_E \in G$, $\alpha_i \neq \alpha_j$ for all $i \neq j$ and $k \leq |G|$. The polynomial $q_\alpha = (x - \alpha_1) \ldots (x - \alpha_k) \in E[x]$ has no multiple roots, and $q_\alpha(\alpha) = 0$. Every automorphism $\tau \in G$ maps roots of q_α to roots of q_α: for any $\alpha_i = \sigma(\alpha)$ for some $\sigma \in G$, $\tau\sigma(\alpha) = \alpha_j$ for some j, as $\tau\sigma = \sigma \circ \tau \in G$. τ fixes q_α, hence $q_\alpha \in F[x]$. The extension E/F is algebraic, and the minimal polynomial of α over F exists by 3.2, and it divides q_α, so it does not have any multiple roots and E/F is separable and $[F(\alpha) : F] \leq \deg(q_\alpha) \leq |G|$ so by 3.14, E/F is finite and $[E : F] \leq |G|$. All the roots of the minimum polynomial are in E for every α, so $E = F(\{\text{roots of } p_\alpha \mid \alpha \in E\})$ and E/F is normal. E/F is Galois; by 3.13, $|\mathrm{Gal}(E/F)| = [E : F] \leq |G|$ and $G \leq \mathrm{Gal}(E/F)$, so $G = \mathrm{Gal}(E/F)$ since they are both finite. □

We have gathered enough results to prove the Main Theorem for the Finite case

Theorem 3.16. *Let E/K be a finite Galois extension. Let $\mathscr{S} = \{F \text{ field} \mid K \subseteq F \subseteq E\}$ and $\mathscr{R} = \{H \leq Gal(E/K)\}$ and consider $\Phi : \mathscr{S} \to \mathscr{R}$ such that $\Phi(M) = Gal(E/M)$, $\Psi : \mathscr{R} \to \mathscr{S}$ such that $\Psi(H) = E^H$. Then, Φ and Ψ are inverse of each other, and therefore there is an inclusion-reversing bijection between the set of between fields of the Galois extension E/K and the set of subgroups of $Gal(E/K)$.*

Proof. Φ and Ψ being inverses of each other means proving that $E^{\mathrm{Gal}(E/M)} = M$ and $\mathrm{Gal}(E/E^H) = H$ for every $H \leq \mathrm{Gal}(E/K)$ and $K \subseteq M \subseteq E$. E/K is Galois, so E/M is Galois, by 3.13, $E^{\mathrm{Gal}(E/M)} = M$ and $|\mathrm{Gal}(E/K)| = [E : K] < \infty$. For every $H \leq \mathrm{Gal}(E/K)$, H is finite because so is $\mathrm{Gal}(E/K)$ and by 3.15, $H = \mathrm{Gal}(E/E^H)$. □

3.2 The Krull Topology on Gal(E/K).

Consider E a field and K a subfield of E, E/K be a possibly infinite Galois extension. We will now continue further and extend the main theorem for finite extensions to the infinite case, referring to a topology we will soon define in the Galois groups, called Krull's topology. In particular, we will bring here a connection between Galois groups on infinite extensions and the Profinite Groups Theory. First of all, consider the family of subfields of E:

$$\mathscr{F} = \{L \mid L \text{ subfield of } E \text{ such that the extension } L/K \text{ is Galois and finite}\}$$

We define a topology on $\mathrm{Gal}(E/K)$ by considering as a base of open neighborhoods for Id_E the family $\mathscr{N}$ of subgroups of $\mathrm{Gal}(E/K)$, where $\mathscr{N} = \{\mathrm{Gal}(E/L) \mid L \in \mathscr{F}\}$. This topology is commonly called *The Krull topology* or *the finite topology* on $\mathrm{Gal}(E/K)$[1]. This family meets the requirements to form a basis of a certain topology:

(i) the union of all the elements in $\mathscr{N}$ is $\mathrm{Gal}(E/K)$: Since K/K is trivially finite and Galois, $K \in \mathscr{F}$ and $\mathscr{F} \neq \emptyset$, and $\mathrm{Gal}(E/K) \subseteq \cup_{L \in \mathscr{F}} \mathrm{Gal}(E/L)$. Trivially all the subfields of E in $\mathscr{F}$ contain K, so $\cup_{L \in \mathscr{F}} \mathrm{Gal}(E/L) = \mathrm{Gal}(E/K)$.

(ii) The double intersection of two of these Galois groups is also a union of elements in $\mathscr{N}$: For $L_1, L_2 \in \mathscr{F}$, $L_1/K, L_2/K$ are both finite, Galois and $\mathrm{Gal}(E/L_1) \cap \mathrm{Gal}(E/L_2) = \mathrm{Gal}(E/L_1L_2)$ where $L_1L_2 = L_1(L_2).L_1/K$, L_2/K are both normal and fiinte, and the composition L_1L_2/K is separable, normal and finite. For details, see [3]. In particular, $L_1L_2 \in \mathscr{F}$ and $\mathrm{Gal}(E/L_1L_2)$ is a basic open neighborhood of Id_E.

[1] More generally, one can define the Krull topology as follows: for X and Y two sets and M a set of mappings between X and Y, S a finite subset of X and $f \in M$, the sets $V(f,S) = \{g \in M \mid g(s) = f(s)\ \forall s \in S\}$ are a well defined family of neighborhoods of each $f \in M$ and in the particular case of $\mathrm{Gal}(E/K)$, they are essentially the family $\mathscr{N}$ presented above.

This all ends up in stating that $\mathrm{Gal}(E/K)$ is a topological group and the group operations are continuous in the generated topology: For the product defined via $\alpha\beta = \beta \circ \alpha$, let $\sigma, \tau \in \mathrm{Gal}(E/K)$. For every open neighborhood $\sigma\tau \in U \subseteq \mathrm{Gal}(E/K)$, there is a subfield $L \in \mathscr{F}$ such that L/K is Galois and finite, In particular the extension is normal, and $\sigma(L) = L, \tau(L) = L$ by 3.12. Moreover, $\sigma\tau \in \sigma\tau\mathrm{Gal}(E/L) \subseteq U$ and the image of $\sigma\mathrm{Gal}(E/L) \times \tau\mathrm{Gal}(E/L)$ via the product is contained in U, so the product in $\mathrm{Gal}(E/K)$ is continuous. For the inversion, for every $\sigma^{-1} \in \mathrm{Gal}(E/L)\sigma^{-1} \subseteq U$, the inversion maps $\sigma\mathrm{Gal}(E/L)$ to $\mathrm{Gal}(E/L)\sigma^{-1}$ and the continuity holds.

Remark. From the beginning, we allowed the possibility of E/K being infinite. Even so, for the finite case, $\mathscr{F}$ is formed by all the intermediate fields in E/K and in accordance with the Main theorem for Galois extensions from 3.16, the **only** subgroups of $\mathrm{Gal}(E/K)$ are the subgroups belonging to $\mathscr{N}$ (and $\mathscr{N}$ has them all). Additionally, since E/K is Galois, for every L such that $K \subseteq L \subseteq E$, E/L is Galois and $|\mathrm{Gal}(E/L)| = [E : L] < \infty$ so all these subgroups are finite, included $\mathrm{Gal}(E/K)$. There is a finite number of intermediate fields between K and E, so $\mathscr{F}$ is finite and the intersection

$$\bigcap_{L\in\mathscr{F}} \mathrm{Gal}(E/L)$$

is an open set. That intersection contains $\mathrm{Gal}(E/E)$, which is trivial, since $E \in \mathscr{F}$, and it equals $\{\mathrm{Id}_E\}$. All the Galois groups $\mathrm{Gal}(E/K)$ when E/K is finite are also finite and, moreover, discrete.

3.2.1 Inverse Systems of Galois Groups.

First of all, we begin with some technical results in finite extensions which are going to be of importance in further proof details.

Remark. The family $\mathscr{F}$ inherits a poset structure: for every $L_1, L_2 \in \mathscr{F}$, $L_1 \leq L_2$ if and only if L_1 is a subfield of L_2. Notice that for every $L_1, L_2 \in \mathscr{F}$, $L_1L_2 \in \mathscr{F}$ and $L_1, L_2 \leq L_1L_2$. The rest of properties of the posets follow immediately, as $L_1 \leq L_2$ implies in particular that $L_1 \subseteq L_2$. Constructing a family of maps $\{\varphi_{L_2L_1}\}_{L_1\leq L_2}$, where

$$\begin{aligned} \varphi_{L_2L_1} \colon \mathrm{Gal}(L_2/K) &\to \mathrm{Gal}(L_1/K) \\ \sigma &\mapsto \sigma|_{L_1} \end{aligned}$$

We have that as a particular case of 3.11, every isomorphism in $\mathrm{Gal}(L_1/K)$ has an extension to L_2 and $\varphi_{L_2L_1}$ is an epimorphism and also continuous since both spaces are discrete given that L_1/K and L_2/K are finite and Galois extensions. Notice that L_1/K is in particular normal and L_1 is a subfield of L_2, so $\sigma(L_1) = L_1$ for every $\sigma \in \mathrm{Gal}(L_2/K)$. For every $L_1 \leq L_2 \leq L_3$, $\varphi_{L_3L_1}(\sigma) = \sigma|_{L_1} = \sigma|_{L_2}|_{L_1} = \varphi_{L_2L_1} \circ \varphi_{L_3L_2}(\sigma)$. As a result, $\{\mathrm{Gal}(L/K), \varphi_{L_1L_2}, L \in \mathscr{F}\}$ forms an inverse system over $\mathscr{F}$.

Proposition 3.17. *Let E/K be a Galois extension. Considering the same inverse system as before, $Gal(E/K)$ is the inverse limit of the finite groups $Gal(L/K)$ where $L \in \mathscr{F}$; as a consequence, $Gal(E/K)$ is a profinite group.*

Proof. Here, we are going to prove the isomorphism of $\mathrm{Gal}(E/K)$ with $\varprojlim_{L\in\mathscr{F}} \mathrm{Gal}(L/K)$ where the inverse limit is considered together with the canonical projections between $\prod_{L\in\mathscr{F}} \mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/K)$ for each $L \in \mathscr{F}$. Also, since $L \leq E$ for every $L \in \mathscr{F}$, L/K is finite and Galois, in particular is normal so the restriction mappings from $\mathrm{Gal}(E/K)$ to $\mathrm{Gal}(L/K)$ that map every $\sigma \in \mathrm{Gal}(E/K)$ to $\sigma|_L$ are well defined, in accordance with 3.12. Thus, extending these restriction maps to the direct product over all elements in $\mathscr{F}$, let φ be

$$\begin{aligned} \varphi \colon \mathrm{Gal}(E/K) &\to \prod_{L\in\mathscr{F}} \mathrm{Gal}(L/K) \\ \sigma &\mapsto (\sigma|_L)_{L\in\mathscr{F}} \end{aligned}$$

For every two subfields $L_1 \leq L_2$ in $\mathscr{F}$, $\varphi_{L_2L_1}(\sigma|_{L_2}) = \sigma|_{L_1 \cap L_2} = \sigma|_{L_1}$. The image of φ under $\mathrm{Gal}(E/K)$ is contained in $\varprojlim_{L\in\mathscr{F}} \mathrm{Gal}(L/K)$. Also, φ is a group homomorphism: for every two $\sigma, \tau \in \mathrm{Gal}(E/K)$, $\varphi(\sigma \circ \tau) = ((\sigma \circ \tau)|_{L\in\mathscr{F}}) = (\sigma|_L) \circ (\tau|_L) = \varphi(\sigma) \circ \varphi(\tau)$ by 3.12 and our definition of the componentwise composition in direct products. Moreover, φ is injective: let $\sigma \in \mathrm{Gal}(E/K)$ such that $\varphi(\sigma) = 1$, then $\sigma|_L = \mathrm{Id}_L$ for all $L \in \mathscr{F}$; let $\alpha \in E$, and p the irreducible polynomial of α in $K[x]$, p is irreducible and has a root α in E; E/K is normal, p is irreducible and by 3.9 $X_\alpha \equiv \{\text{roots of } p\} \subseteq E$. The extension $K(X_\alpha)/K$ is normal since it is the splitting field of p and separable since E/K is separable, $K(X_\alpha)/K$ is Galois, finite and it contains $K(\alpha)$, so $K(X_\alpha) \in \mathscr{F}$ and $\sigma(\alpha) = \sigma|_{K(X_\alpha)}(\alpha) = \alpha$ and $\sigma = \mathrm{Id}_E$. The image of φ is furthermore $\varprojlim_{L\in\mathscr{F}} \mathrm{Gal}(L/K)$: for every $(\sigma_L)_{L\in\mathscr{F}} \in \varprojlim \mathrm{Gal}(L/K)$, we define an automorphism of E as follows: let $\alpha \in E$, $K(X_\alpha)$ considered as above, $\sigma(\alpha) := \sigma_{K(X_\alpha)}(\alpha)$; σ does not depend on the field chosen in the role of $K(X_\alpha)$; for another field $M \in \mathscr{F}$ such that $K(\alpha) \subseteq M$ providing that $\mathscr{F}$ is a poset, there exists $F \in \mathscr{F}$ such that $M, K(X_\alpha) \leq F$ and by the compatibility with the maps defining the inverse system, $\varphi_{FM}(\sigma_F) = \sigma_F|_M = \sigma_M$ and $\varphi_{FK(X_\alpha)}(\sigma_F) = \sigma_F|_{K(X_\alpha)} = \sigma_{K(X_\alpha)}$ so $\sigma_M(\alpha) = \sigma_F(\alpha) = \sigma_{K(X_\alpha)}(\alpha)$. We have that $\sigma \in \mathrm{Gal}(E/K)$: it fixes K elementwise, it is injective and surjective as σ_L are field isomorphisms and it preserves the field operations in E: $\sigma(\alpha+\beta) = \sigma_{K(X_{\alpha+\beta})}(\alpha+\beta) = \sigma_{K(X_\alpha)(K(X_\beta))}(\alpha) + \sigma_{K(X_\alpha)(K(X_\beta))}(\beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ analogously, $\varphi(\sigma) = (\sigma_L)$ by definition of σ.

It remains to show that φ is an isomorphism of topological groups. For that, take into account that for each $N \in \mathscr{F}$, $\mathrm{Gal}(E/N)$ is a basic neighborhood of Id_E and

$$\varphi(\mathrm{Gal}(E/N)) = \{(\sigma_L) \in \varprojlim_{L\in\mathscr{F}} \mathrm{Gal}(L/K) \mid \sigma_N = \mathrm{Id}_N\ \}$$

These are the kernels of the canonical projections intersected with $\varprojlim$ $\mathrm{Gal}(L/K)$, and by 2.1, they form a fundamental system for Id_E and φ maps a basis of neighborhoods of Id_E to another basis. The basis of neighborhoods for Id_E is moreover formed by images of basic open sets of $\mathscr{F}$, so φ is an homeomorphism, and $\mathrm{Gal}(E/K) \cong \varprojlim_{L\in\mathscr{F}} \mathrm{Gal}(L/K)$ as topological groups.

□

Now we can deduce all the consequences we have been dealing with in the past sections, specially concerning with the topological structure of $\mathrm{Gal}(E/K)$.

Corollary 3.18. *Let E/K be a possibly Galois infinite extension, and consider Gal(E/K) with the Krull Topology. Then, Gal(E/K) is compact, Hausdorff and totally disconnected.*

Proof. By 3.17, $\mathrm{Gal}(E/K)$ is a profinite group; by 2.3, $\mathrm{Gal}(E/K)$ is compact, Hausdorff and totally disconnected. □

Proposition 3.19. *Let M_1 and M_2 be between fields of the Galois extension E/K and let $\gamma : M_1 \to M_2$ be a field isomorphim that fixes K elementwise. Then γ can be extended to an automorphism of E.*

Proof. Let $N \in \mathscr{F}$ and B_N the subset of $\prod_{L\in\mathscr{F}} \mathrm{Gal}(L/K)$ defined in the following terms:

$$B_N = \left\{ (\sigma_L) \in \prod_{L\in\mathscr{F}} \mathrm{Gal}(L/K) \mid \sigma_N|_{N\cap M_1} = \gamma|_{N\cap M_1} \text{ and } \sigma_L = \sigma_N|_L \text{ for } L \leq N \right\}$$

γ is a field isomorphism, restricting γ to $N \cap M_1$, $\gamma|_{N\cap M_1} : N \cap M_1 \to \gamma(N \cap M_1)$ is a field isomorphism that fixes every element of K and N/K is finite and Galois. In particular, N/K is normal, so by 3.7, N/K is algebraic. For every $a \in N \cap M_1$, since $a \in N$, there exists a monic irreducible polynomial $p \in K[x]$ such that $p(a) = 0$ by 3.2, and $a \in M_1$. Applying 3.9, N contains all the roots of p, and γ fixes K element by element, so $\gamma(a)$ is another root of p and $\gamma(a) \in N \cap M_2$, so $\gamma(N \cap M_1) \subseteq N \cap M_2$ and by an analogous argument, $\gamma(N \cap M_1) = N \cap M_2$. Applying 3.11, there exists an automorphism $\sigma_N : N \to N$ that extends $\gamma|_{N\cap M_1}$ and therefore fixes K elementwise, so $\sigma_N \in \mathrm{Gal}(N/K)$. The sequence $(\sigma_L)_{L\in\mathscr{F}}$ where

$$\sigma_M = \begin{cases} \sigma_N|_M & \text{if } \ M \leq N \\ \mathrm{Id}_M & \text{if } \ M \nleq N \end{cases}$$

for each $M \in \mathscr{F}$ lies in B_N so for every $N \in \mathscr{F}$, $B_N \neq \emptyset$. For every $L \in \mathscr{F}$, L/K is finite and Galois, so $\mathrm{Gal}(L/K)$ is finite and discrete as we argued in 3.2. Thus, every subset of $\mathrm{Gal}(L/K)$ is closed, and rewriting B_N as

$$B_N = \left[\prod_{L\in\mathscr{F}\setminus N} \mathrm{Gal}(L/K) \times \{\sigma_N \in \mathrm{Gal}(N/K) \mid \sigma_N|_{N\cap M_1} = \gamma|_{N\cap M_1}\}\right] \cap \{(\sigma_L) \mid \sigma_L = \varphi_{NL}(\sigma_N)\ L \leq N\}$$

B_N is intersection of two closed sets, the first one since it is the product of all the groups $\mathrm{Gal}(L/K)$ except the single case in which $L = N$, and the second one by the proof argument in 1.5. For every two fields $N_1, N_2 \in \mathscr{F}$, $N_1N_2 \in \mathscr{F}$, as we explained in §3.2. Then, $B_{N_1N_2} \subseteq B_{N_1} \cap B_{N_2}$: for every $(\sigma_L) \in B_{N_1N_2}$, $\sigma_{N_i} = \sigma_{N_1N_2}|_{N_i}$ for $i = 1, 2$ and every subfield of N_1 or N_2 is subfield of N_1N_2, so $B_{N_1N_2} \subseteq B_{N_1} \cap B_{N_2}$ and inductively, every finite intersection of the sets B_N is nonempty. The sets B_N are closed and subsets of compact spaces as for all $L \in \mathscr{F}$, $\mathrm{Gal}(L/K)$ is finite and discrete, so compact, and B_N is compact for every $N \in \mathscr{F}$. By the finite intersection property, $B = \bigcap_{N\in\mathscr{F}} B_N \neq \emptyset$, and $B \subseteq \varprojlim_{L\in\mathscr{F}} \mathrm{Gal}(L/K)$. Then, a map in $\varphi^{-1}(B) \neq \emptyset$, where φ is the map from 3.17, extends γ: for $\sigma \in \varphi^{-1}(B)$, $\sigma|_{N\cap M_1} = \gamma|_{N\cap M_1}$ for all $N \in \mathscr{F}$, so $\sigma|_{M_1} = \gamma$, as M_1 is maximal in $\{N \cap M_1 \mid N \in \mathscr{F}\}$. [2] □

Lemma 3.20. *Let E/K be Galois. Suppose that $E = \bigcup_{i\in I} E_i$ where each E_i is a finite extension of K contained in E. Then $\{Gal(E/E_i) \mid i \in I\}$ is a base of open neighborhoods of Id_E in $Gal(E/K)$.*

Proof. Consider $i \in I$ fixed, E_i/K is finite so it is algebraic, and moreover, there exist $\alpha_1, \ldots, \alpha_s \in E_i$ such that $E_i = K\langle\alpha_1, \ldots, \alpha_s\rangle$. E/K is Galois, in particular it is normal, so it is algebraic by 3.7. Let p_{α_i} be the minimal polynomial of each α_i. E/K is normal, by 3.9, E contains the set of roots of each p_{α_i}, denoted as X_{α_i}, for $i = 1, \ldots, s$. Then, $K(X_{\alpha_i} \mid i = 1, \ldots, s)$ contains E_i, and it is normal and finite over K since it is a finitely generated field by algebraic elements. It is also separable since so is E/K, and $K(X_{\alpha_i} \mid i = 1, \ldots, s)$ is Galois over K and finite, so it belongs to $\mathscr{F}$. Thus, for each E_i there exist $N \in \mathscr{F}$ such that $E_i \subseteq N$. Since $E_i \subseteq N$, $\mathrm{Gal}(E/N) \leq \mathrm{Gal}(E/E_i)$ and for every $i \in I$, $\mathrm{Gal}(E/E_i)$ is open: $\mathrm{Gal}(E/E_i)$ is a subgroup of $\mathrm{Gal}(E/K)$ and it contains an open subgroup $\mathrm{Gal}(E/N)$, so $\mathrm{Gal}(E/E_i) = \bigcup_{\sigma\in\mathrm{Gal}(E/E_i)} \sigma\mathrm{Gal}(E/N)$ open by union of open sets. Conversely, if $N \in \mathscr{F}$, then N/K is finite and Galois. In particular it is separable and finite, by 3.6, there exists $\alpha \in N$ such that $N = K(\alpha)$. Since E is the union of all E_i, and $\alpha \in E$, there is some $j \in I$ such that $\alpha \in E_j$ and $N = K(\alpha) \leq E_j$ so $\mathrm{Gal}(E/E_j) \leq \mathrm{Gal}(E/N)$. Therefore, the family $\{\mathrm{Gal}(E/E_i) \mid i \in I\}$ generates the same topology as $\{\mathrm{Gal}(E/N) \mid N \in \mathscr{F}\}$. □

Proposition 3.21. *Let M be a between field of the Galois extension E/K. The topology of the subgroup $Gal(E/M)$ is induced as the subspace topology on $Gal(E/K)$, and $Gal(E/M)$ is a* ***closed*** *subgroup of $Gal(E/K)$.*

Proof. The subspace topology induced on $\mathrm{Gal}(E/M)$ has a base of neighborhoods of Id_E given by the intersection with the basic neighborhoods in $\mathscr{N}$, i.e. $\{\mathrm{Gal}(E/M) \cap \mathrm{Gal}(E/L) \mid L \in \mathscr{F}\}$. Since for each $L \in \mathscr{F}$, $\mathrm{Gal}(E/M) \cap \mathrm{Gal}(E/L) = \mathrm{Gal}(E/LM)$, the induced topology on $\mathrm{Gal}(E/M)$ has a base of neighborhoods for the identity $\{\mathrm{Gal}(E/LM) \mid L \in \mathscr{F}\}$. Applying together 3.17 and 3.18 $\mathrm{Gal}(E/M)$ is a profinite group and in particular compact, it is a compact subspace of $\mathrm{Gal}(E/K)$, which is also by 3.18 compact, Hausdorff and totally disconnected, so particularly since it is a compact subspace of a Hausdorff space, it is closed, and $\mathrm{Gal}(E/M)$ is a closed subgroup of $\mathrm{Gal}(E/K)$. □

[2] Applying Zorn's Lemma in the set $\{N \cap M_1 \mid N \in \mathscr{F}\}$ we have that there is a maximal set $N^* \cap M_1$ which has to be equal to M_1; if it was not, there would exist $x \in M_1 \setminus N^*$ and we could take a bigger extension of K in $\mathscr{F}$ that contains N^*, which will be $N^*(x)$.

3.2.2 The Krull Theorem

Here, we arrive to the extension we referred to in the previous parts, concerning to the extension of the Main Theorem of Galois Theory now on possible infinite Galois extensions. We will characterize, again, the subgroups of $\mathrm{Gal}(E/K)$.

Theorem 3.22. *Let E/K be a Galois extension. Then, the map Φ defined by $\Phi(M) = Gal(E/M)$ is an inclusion-reversing bijection from the set of between fields M of the extension E/K to the set of* ***closed*** *subgroups of $Gal(E/K)$. Its inverse Φ^{-1} maps each subgroup H of $Gal(E/K)$ to the fixed field E^H of all elements in E fixed by H.*

Proof. Denote $\mathscr{S} = \{F \text{ field } \mid K \subseteq F \subseteq E\}$ and $\mathscr{K} = \{H \leq \mathrm{Gal}(E/K) \mid H \text{ closed}\}$, $\Phi : \mathscr{S} \to \mathscr{K}$ and let $\Psi : \mathscr{K} \to \mathscr{S}$ such that $\Psi(H) = E^H$, in order to prove that Φ is a bijection and that its inverse is indeed Ψ, we are going to prove that $\Psi \circ \Phi = \mathrm{Id}_{\mathscr{S}}$, and $\Phi \circ \Psi = \mathrm{Id}_{\mathscr{K}}$. As first remarks, notice that for every between field M in the extension E/K, if M is generated by subfields $\{M_i \mid i \in I\}$, that is, $M = K(M_i \mid i \in I)$, then $\mathrm{Gal}(E/M) = \bigcap_{i\in I} \mathrm{Gal}(E/M_i)$. On the other hand, for every $\alpha \in E$, the extension $K(\alpha)/K$ is finite by 3.7 and 3.8. Given that

$$E = \bigcup_{\alpha \in E} K(\alpha)$$

by 3.20, $\{\mathrm{Gal}(E/K(\alpha)) \mid \alpha \in E\}$ is a base of open neighborhoods for Id_E in $\mathrm{Gal}(E/K)$, and if some M_i is a finite extension of K, there are some $\alpha_1, \ldots, \alpha_r$ such that $M_i = K(\alpha_1, \ldots, \alpha_r)$ and $\mathrm{Gal}(E/M_i) = \bigcap_{i=1}^{r} \mathrm{Gal}(E/K(\alpha_i))$ that is, a finite intersection of basic open neighborhoods, so $\mathrm{Gal}(E/M_i) \leq \mathrm{Gal}(E/K)$ is open. By 3.21, $\mathrm{Gal}(E/M_i)$ is a closed subgroup of $\mathrm{Gal}(E/K)$, so if M is generated by all the M_i, then $\mathrm{Gal}(E/M)$ is a closed subgroup by intersection. As we have observed before, Φ is inclusion-reversing since for every two between fields of the extension E/K, $M_1 \leq M_2$, then Φ reverses the order relation, i.e., $\mathrm{Gal}(E/M_1) \geq \mathrm{Gal}(E/M_2)$ and $\Phi(M_1) \geq \Phi(M_2)$.

Let M be a between field in E/K, let us see that $\Psi \circ \Phi(M) = M$, i.e., $M = E^{\mathrm{Gal}(E/M)}$. By hypothesis E/K is Galois, so for every between field M, so is E/M and by 3.13, we prove the claim and $E^{\mathrm{Gal}(E/M)} = M$. To see that $\Phi \circ \Psi = \mathrm{Id}_{\mathscr{K}}$, let H be a subgroup of $\mathrm{Gal}(E/K)$, we must prove that $H = \mathrm{Gal}(E/E^H)$. It suffices to show that $H = \mathrm{Gal}(E/M)$ for some between field $M \in \mathscr{S}$, as we have already proved that if $H = \mathrm{Gal}(E/M)$, then $E^H = E^{\mathrm{Gal}(E/M)} = M$. We are going to restrict H to be open: by 3.18, $\mathrm{Gal}(E/K)$ is in particular compact, so every open subgroup of $\mathrm{Gal}(E/K)$ has finite index by 2.2. Also, every open subgroup of $\mathrm{Gal}(E/K)$ is closed, and every closed subgroup of finite index is open. Also, if H is closed, then H is an intersection of basic neighborhoods, and Φ is closed under intersections in the sense explained above, that is, the intersection of Galois groups images through Φ is another Galois group and the intersection still lies in the image of Φ, via the composition field; there is no loss of generality then if we set that $H \leq \mathrm{Gal}(E/K)$ is open. Since $\mathscr{N}$ is a base of open neighborhoods of $\mathrm{Gal}(E/K)$ for Id_E, there exists some $L \in \mathscr{F}$ such that L/K is finite, Galois, and $\mathrm{Gal}(E/L) \leq H$. Moreover, L/K is in particular normal, so by 3.12, for every $\sigma \in \mathrm{Gal}(E/K)$, $\sigma(L) = L$ and the set $H_L = \{\sigma|_L : \sigma \in H\}$ is a subgroup of $\mathrm{Gal}(L/K)$; L/K is finite and Galois, applying the Main Theorem of Galois Theory for the finite case in 3.16, $H_L = \mathrm{Gal}(L/L^{H_L})$ and let $M = L^{H_L}$, we claim that $H = \mathrm{Gal}(E/L^{H_L}) = \mathrm{Gal}(E/M)$: First, for every $\sigma \in H$, then $\sigma|_L \in H_L$ and σ is an automorphism of E that fixes every element in M by construction: indeed, for every $\alpha \in M$, $\sigma(\alpha) = \sigma|_L(\alpha) = \alpha$ and $H \leq \mathrm{Gal}(E/L^{H_L})$.

Conversely, for every $\sigma \in \mathrm{Gal}(E/L^{H_L})$, as we know $\sigma|_L$ is an automorphism of L given that L/K is Galois and finite, and $\sigma|_L \in \mathrm{Gal}(L/L^{H_L}) = H_L$, so there exists $\tau \in H$ such that $\sigma|_L = \tau|_L$ and $\tau^{-1}\sigma$ is the identity in L, that is, $\tau^{-1}\sigma \in \mathrm{Gal}(E/L) \leq H$ so $\tau^{-1}\sigma \in H$ and $\sigma = \tau\tau^{-1}\sigma \in H$, $H = \mathrm{Gal}(E/M)$ and the rest holds. □

3.3 Profinite Groups as Galois Groups.

Lemma 3.23. *Let θ be a not necessarily continuous homomorphism from a profinite group G to the Galois group of a field extension E/K. For each $\alpha \in E$ write $G_\alpha := \{g \in G \mid \theta(g)(\alpha) = \alpha\}$. Assume that G_α is open for each $\alpha \in E$ and that $E^{\theta(G)} = K$. Then, E/K is Galois, and θ is continuous and surjective.*

Proof. Consider G profinite and assume G_α is open for every $\alpha \in E$. Let R_α be, for each $\alpha \in E$, the *core* over G of the subgroup $G_\alpha \leq G$, that is

$$R_\alpha = \bigcap_{g \in G} g^{-1} G_\alpha g$$

By hypothesis, G_α is a subgroup of a profinite group, so by 2.3, since $1_G \in G_\alpha$ for all $\alpha \in E$, there exists an open normal subgroup of G such that $N \trianglelefteq G_\alpha$ and G/N is finite and discrete. Also, since N is normal, for every $g \in G$, $g^{-1}Ng = N$, so accordingly $N \leq g^{-1}G_\alpha g$ for every $g \in G$ and $N \trianglelefteq R_\alpha$. N is an open normal subgroup, $R_\alpha = \bigcup_{a \in R_\alpha} aN$, union of open sets, so R_α is open, and normal as $h^{-1}R_\alpha h = R_\alpha$ for every $h \in G$. Let $x_1, \dots, x_r \in E$, and L be the subfield of E such that $L = K(\theta(g)(x_1), \dots, \theta(g)(x_r) \mid g \in G)$. For every $g, h \in G, 1 \leq i \leq r$, $\theta(g)(\theta(h)(x_i)) = \theta(g) \circ \theta(h)(x_i) = \theta(gh)(x_i)$ and for every $g \in G$, $\theta(g)(L) \subseteq L$; moreover, $\{\theta(g)(x_1), \dots, \theta(g)(x_r)\} \subseteq \theta(g)(L)$ as $x_1, \dots, x_r \in L$, so $\theta(g)(L) = L$ and G acts via θ in $\mathrm{Gal}(L/K)$. For every $g \in G$, $\theta(g)|_L$ is an automorphism of L that fixes K as so does $\theta(g)$ and $K \subseteq L$. Define the map

$$\begin{aligned} \psi \colon G &\to \mathrm{Gal}(L/K) \\ g &\mapsto \theta(g)|_L \end{aligned}$$

ψ is a group homomorphism given that so is θ, and ψ is well defined since restricting $\theta(g)$ to L yields to another automorphism of L that fixes K as $\theta(g)$ belongs to $\mathrm{Gal}(E/K)$. Every $g \in G$ such that $\theta(g)|_L = \mathrm{Id}_L$, fulfills that for every $x_i, 1 \leq i \leq r$ and $h \in G$, $\theta(g)(\theta(h)(x_i)) = \theta(h)(x_i)$ and $\theta(gh)(x_i) = \theta(h)(x_i)$; as θ is a homorphism, $\theta(g^{-1}) = \theta(g)^{-1}$ consequently $\theta(h^{-1}gh)(x_i) = x_i$ and $h^{-1}gh \in G_{x_i}$ for every $1 \leq i \leq r$ and $h \in G$, so $g \in R_{x_1} \cap \dots \cap R_{x_r}$, Ker $\psi = R_{x_1} \cap \dots R_{x_r}$ normal and open by intersection. We assumed that G is profinite, and Ker ψ is an open and normal subgroup of G, $G/$Ker ψ is finite and discrete by 2.3. Applying the isomorphism theorem

$$G/R_{x_1} \cap \cdots R_{x_r} \cong \mathrm{Im}\ \psi$$

As a result, $\theta(G)|_L := \mathrm{Im}\ \psi = \{\theta(g)|_L \mid g \in G\} \leq \mathrm{Gal}(L/K)$ is finite. $\theta(G)|_L$ is a finite subgroup of automorphisms of the field L, by 3.15, L is a finite Galois extension of $L^{\theta(G)|_L}$ and $\mathrm{Gal}(L/L^{\theta(G)|_L}) = \theta(G)|_L$. As $E^{\theta(G)} = K$, $L^{\theta(G)|_L} = K$ and L/K is finite and Galois. E is a union of fields constructed like L, more concretely

$$E = \bigcup_{\alpha \in E} K(\theta(g)(\alpha) \mid g \in G)$$

and each field $L_\alpha = K(\theta(g)(\alpha) \mid g \in G)$ is an extension of K that is finite and Galois, by union E/K is normal and separable because so are all the L_α. E/K is consequently a Galois extension. Let us see that θ is continuous: it suffices to show that for every $F \in \mathscr{F}$ and basic neighborhood $\mathrm{Gal}(E/F)$ of Id_E, $\theta^{-1}(\mathrm{Gal}(E/F))$ is open in G. First, for each $F \in \mathscr{F}$, $\theta^{-1}(\mathrm{Gal}(E/F)) = \{g \in G \mid \theta(g)(a) = a, \forall a \in F\}$ which is expressed, in terms of the sets G_α,

$$\theta^{-1}(\mathrm{Gal}(E/F)) = \bigcap_{a \in F} G_a$$

G is profinite, by 2.3 is compact, and by 2.2 every open subgroup of G is open if and only if it is closed and has finite index. Since all the G_a are open, they are closed, and the intersection $\cap_{a \in F} G_a$ is closed, so we only have to check that it has finite index with respect to G. For that purpose, consider the map:

$$\begin{aligned} \phi \colon G &\to \mathrm{Gal}(F/K) \\ g &\mapsto \theta(g)|_F \end{aligned}$$

analogous as before; F/K is finite and Galois, so $\mathrm{Gal}(F/K)$ is finite and its order is $[F:K]$ by 3.13. In particular, F/K is normal, so $\theta(g)|_F$ is well defined as an automorphism of F that fixes K. Similarly,

$$\mathrm{Ker}\,\phi = \{g \in G \mid \theta(g)(\alpha) = \alpha \;\forall \alpha \in F\} = \bigcap_{\alpha \in F} G_\alpha \trianglelefteq G$$

and by the isomorphism theorem, $G/\bigcap_{\alpha \in F} G_\alpha \cong \mathrm{Im}\,\phi \leq \mathrm{Gal}(F/K)$ and $\theta^{-1}(\mathrm{Gal}(E/F))$ is closed and has finite index, so it is open, and θ is continuous. To see the surjectivity: as G is profinite, in particular it is compact, and $\theta(G)$ is compact in $\mathrm{Gal}(E/K)$, which is Hausdorff as it is also profinite, so $\theta(G)$ is a closed subgroup of $\mathrm{Gal}(E/K)$. By 3.22, $\theta(G) = \mathrm{Gal}(E/E^{\theta(G)}) = \mathrm{Gal}(E/K)$. □

We reach the goal of the thesis, proving that profinite groups and Galois groups with the Krull topology are, indeed, indistinguishable up to isomorphism of topological groups, as the following theorem claims.

Theorem 3.24. *Every profinite group is isomorphic (as a topological group) to a Galois group.*

Proof. Let K be a field, and assume that G is profinite. By 2.3 there exists a fundamental system $\mathscr{N}$ of open normal subgroups of G such that $\bigcap_{N \in \mathscr{N}} N = 1$ and G/N is finite and discrete for every $N \in \mathscr{N}$; denote

$$S = \bigcup_{N \in \mathscr{N}} G/N$$

and

$$E = K(X_s \mid s \in S)$$

where $\{X_s\}_{s \in S}$ is an algebraically independent family over K, that is, there is no $f \in K[X_s \mid s \in S]$ such that $f((X_s)_{s \in S}) = 0$. Equivalently, E can be seen as the field of fractions of $K[X_s \mid s \in S]$, the ring of polynomials with variables indexed by S. Firstly, S is a G-set, that is, G acts on S under an action $\Phi : G \times S \to S$ defined by $\Phi(g, hN) \equiv g \cdot (hN) := (gh)N$. Φ is a well defined action, as $\Phi(1_G, hN) = hN$ and $\Phi(g_1 g_2, hN) = (g_1 g_2 h)N = \Phi(g_1, \Phi(g_2, hN))$ and for every two classes $gN = hN$, then $gh^{-1} \in N$, $g_1 \cdot (gN) = (g_1 g)N$, $g_2 \cdot (hN) = (g_2 h)N$ which leads to $g_1 gN = g_2 hN$ as $g g_1 g_2^{-1} g^{-1} \in N$, since $N \trianglelefteq G$.

Every element in G defines a bijective map $g \cdot - : S \to S$ given by $g \cdot \sigma N = \Phi(g, \sigma N) = (g\sigma)N$, since it has an inverse $g^{-1} \cdot -$, and G acts on $\{X_s \mid s \in S\}$ by extension of the action on S, via $g \cdot X_s = X_{g \cdot s}$. Extending the action on $\{X_s \mid s \in S\}$ to E to act as a field homomorphism, there is a group homomorphism $\theta : G \to \mathrm{Aut}(E)$ such that $\theta(g) := g \cdot -$ is an automorphism of E for each $g \in G$.

Let $\alpha \in E$, there are $s_1, \ldots, s_r \in S$, $s_i = g_i N_i$, such that $\alpha \in K(X_{s_1}, \ldots, X_{s_r})$, and following the notation of 3.23, the open subgroup by intersection $N_1 \cap \cdots \cap N_r$ is a subgroup of G_α, as for every $g \in N_1 \cap \cdots \cap N_r$, $g \cdot (g_i N_i) = g_i N_i$, for every $1 \leq i \leq r$. G_α is finally open. Let $F = E^{\theta(G)}$, θ can be redefined to be a group homomorphism $\theta : G \to \mathrm{Gal}(E/F)$ and apply 3.23 on θ, it is surjective and continuous. Moreover, θ is injective: for every $g \in G$ that $\theta(g) = \mathrm{Id}_E$, $g \cdot X_s = X_{g \cdot s} = X_s$. By assumption, $\{X_s \mid s \in S\}$ is algebraically independent, therefore $g \cdot s = s$ for all $s \in S$; particularly $g \cdot N = N$ for every $N \in \mathscr{N}$, so $g \in \bigcap_{N \in \mathscr{N}} N$ and $g = 1_G$. Recall that G is profinite, so by 2.3, G is compact, and θ is a bijection with starting space a compact group, θ is a homeomorphism, and $G \cong \mathrm{Gal}(E/F)$. □

Bibliography

[1] L.RIBES AND P.ZALESSKII, *Profinite Groups*, v. **40**, Springer, New York, 2010.

[2] J.S. WILSON, *Profinite Groups*, Clarendon Press, London Mathematical Society Monographs, Oxford, 1998.

[3] P.A. GRILLET, *Abstract Algebra*, Graduate Texts in Mathematics, v. **240**, Second Edition, Springer, New York, 2007.

[4] T. SZAMUELY, *Galois Groups and Fundamental Groups*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2009.

[5] J. LINDELL, *Profinite Groups and Infinite Galois Extensions*, Uppsala University, Algebra and Geometry, Uppsala, Sweden, 2019.

[6] A. ELDUQUE PALOMO, *Groups and Galois Theory*, Course Notes, Departamento de Matemáticas, Universidad de Zaragoza, Zaragoza, 2019.

[7] P. JIMÉNEZ SERAL, *Teoría de Galois*, Departamento de Matemáticas, Universidad de Zaragoza, Zaragoza, 2016.

[8] J. L. NAVARRO, *Topología General*, Departamento de Matemáticas, Universidad de Zaragoza, Zaragoza, 2017.