GALOIS THEORY: A TOPOLOGICAL AND GROUP THEORETIC CONSTRUCTION

by

Taylor Roper

A Thesis Submitted in Partial Fulfillment

of the Requirements for the Degree

Master of Science

Major Subject: Mathematics

West Texas A&M University

Canyon, Texas

April, 2015

ABSTRACT

The definition of the Galois group of any field extension F/K is stated, and the fundamental theorem of Galois theory for algebraic Galois field extensions is proven. Further uncovering the structure of field extensions via their Galois groups, a definiton of the the Krull topology is given that makes the Galois group a topological group that is in fact a profinite group. Topological properties of Galois groups are studied along with the connections these properties have with the corresponding field extensions. A topological characterization of Galois groups of algebraic Galois extensions is then given. The group structure of Galois groups is analyzed via their dependence on and similarities to the structure of finite groups. Most of the main theorems are followed by examples where the theorem is applied to a specific case. The thesis is concluded with a brief discussion of analog Galois theories in other mathematical disciplines.

Table of Contents

1.	Introduction	1
2.	Chapter I The Galois Correspondence	2
3.	Chapter II The Krull Topology	10
4.	Chapter III Profinite Groups: The Structure of Galois Groups	19
5.	Chapter IV A Discussion of Galois Theories Present in Modern Mathematics	30

Introduction

Evariste Galois (1811-1832), a french mathematician, embarked on studying the insolvability of quintic polynomials by radicals. Though a proof was given by Abel in 1824, Galois himself employed ideas that now make up the more modern subject of Galois theory within his proof. His method involved analyzing the group of permutations of the roots of the irreducible polynomials that describe the algebraic extension in order to uncover structure theorems. For example, Galois showed that the insolvability of the group of permutations of the roots of a quintic implies the insolvability of the quintic by radicals. In fact, his proof is what led to the term solvable for the groups having the properties Galois presented. The theory has, for the most part, reached maturity within the subject of fields, and the ideas have been generalized and applied to other distinct mathematical disciplines. In this thesis, I attempt to give a somewhat complete description of Galois groups of infinite dimensional extensions that aid in their calculations and to give an analysis of the topological and group theoretic structure of Galois groups via local considerations. The main theorems presented show that the structure of infinite Galois groups depends on the specific normal subgroups of finite index and that the group is made up of the corresponding quotients.

Chapter I

The Galois Correspondence

Let K be a field and F/K an extension field of K. The dimension of F/K is the dimension of F as a vector space over K and is denoted by $[F : K]$. We denote the Galois group of the extension as $G[F/K] = \{\alpha \in \mathrm{Aut}(F) : \alpha(k) = k \, \forall k \in K\}$. In other words, $G[F/K]$ is all the automorphisms of F that are also K-isomorphisms. The Galois correspondence refers to a bijection between all intermediate fields of the extension and certain subgroups of the group of automorphisms of the field F. In fact, all these subgroups in the correspondence are contained in $G[F/K]$. This is clearly due to the fact that the subgroups in the correspondence are determined by which elements of F they fix and thereby depend upon the vector space structure. We will see this dependence as we develop and discuss the theory. For any subgroup $H < G[F/K]$, let $H' = \{x \in F : \alpha(x) = x \, \forall \alpha \in H\}$. Similarly, for each intermediate field L, let $L' = \{\alpha \in G(F/K) : \alpha(x) = x \, \forall x \in L\} = G[F/L]$. When F is understood, we will denote $G[F/L]$ by $G[L]$. We call H' the fixed field of H. Also, we write $(H')' = H''$ and the same for intermediate fields. We say that a subgroup H of $G[F/K]$ is Galois closed if $H = H''$. Similarly, we say that an intermediate field is Galois if $L'' = L$. In particular, we say that an extension F/K is Galois if $K = K''$, that is, if the fixed field of $G[F/K]$ is precisely K. If an extension F/K is Galois, then for every $\alpha \in G[F/K]$ and $x \in F - K$, $\alpha(x) \in F - K$. In particular, if x is algebraic over K with irreducible polynomial $f \in K[x]$, then $\alpha(x)$ is also a root of f. We exploit this fact in the following theorem.

Theorem 1. *An algebraic extension F/K is Galois if and only if F is a splitting field of a set T of separable polynomials in $K[x]$. More generally, if an extension F/K is Galois, then the subfield E consisting of all the elements in F that are algebraic over K is a splitting field of a set T of separable polynomials in $K[x]$.*

Proof. ($\Rightarrow$) Let $u \in F$ with irreducible polynomial $f \in K[x]$. Let $u = r_1, \ldots, r_n$ be the distinct roots of f that are in F and define $g(x) = (x - r_1) \cdots (x - r_n) \in F[x]$. Since the coefficients of f are in K, then every element of $G[F/K]$ simply permutes the roots of f and hence the roots of g. Thus, the coefficients of g are fixed by every element of $G[F/K]$. Since F/K is Galois, then $g \in K[x]$. The irreducibility of f along with the shared root u of f and g implies that $f \mid g$. Since $\deg g \leq \deg f$ and g is monic, we must have $f = g$. That is, f is separable and splits in F.

Let $\{b_i : i \in I\}$ be a basis of F over K and let f_i be the irreducible polynomial of b_i in $K[x]$. The preceding paragraph implies that each f_i is separable and splits in F. Therefore, F is the splitting field of the set $\{f_i : i \in I\}$ of separable polynomials in $K[x]$.

($\Leftarrow$) Let $u \in F - K$ with irreducible polynomial $f \in K[x]$. Let v be another root of f. Since f is separable and splits in F, $v \neq u$ and $v \in F$. The irreducibility of f gives a K-isomorphism $K(u) \to K(v)$ that maps u to v which extends to a K-isomorphism $\alpha \in G(F/K)$ with $\alpha(u) = v \neq u$ so that F/K is Galois. $\square$

Let K be a field and T the set of all separable polynomials in $K[x]$. A splitting field of T is called the *separable closure* of K and is denoted K^{sep}. Since any two splitting fields of a set of polynomials are isomorphic, K^{sep} is unique up to isomorphism. Also, if F_1/K and F_2/K are two extensions such that $F_1 \cong F_2$, then it is easy to see that $G[F_1/K] \cong G[F_2/K]$. We now can present the following definition.

Definition. Let K be a field and K^{sep} a separable closure of K. The *absolute Galois group* of K, denoted $Gal(K)$, is defined to be $G[K^{sep}/K]$.

We note that for any intermediate field L of an algebraic Galois extension F/K, F/L is always Galois, but L/K may not be as we prove below. L/K is, however, an algebraic separable extension. Thus, L/K is Gaois if and only if it is a splitting field, that is, if every polynomial in $K[x]$ that has a root in L actually splits in

$L[x]$. Hence, L/K is Galois if and only if it is a normal extension. These two facts give us the motivation for Lemma 2 and Theorem 3.

Lemma 2. *Let F/K be an algebraic Galois extension with intermediate field L such that F/L is Galois. Then $G[F/L]$ is normal in $G[F/K]$ if and only if for each $\alpha \in G[F/K]$ and $x \in L$, $\alpha(x) \in L$.*

Proof. Suppose $G[F/L]$ is normal in $G[F/K]$ with F/L Galois. Let $\alpha \in G[F/K]$, $x \in L$, and $\beta \in G[F/L]$. Then $\alpha^{-1}\beta\alpha(x) = x$ so that $\beta\alpha(x) = \alpha(x)$. Hence, $\alpha(x) \in L$ since F/L is Galois.

Conversely, suppose that for each $\alpha \in G[F/K]$ and $x \in L$, $\alpha(x) \in L$. Let $\beta \in G[F/L]$, $\alpha \in G[F/K]$, and $x \in L$. Then $\alpha\beta(x) = \alpha(x)$ so that $\alpha^{-1}\beta\alpha(x) = x$. Again, since F/L is Galois, then $\alpha^{-1}\beta\alpha \in G[F/L]$ whence $G[F/L]$ is normal in $G[F/K]$. □

Theorem 3. *Let F/K be an algebraic Galois extension with intermediate field L. Then F/L is Galois and L/K is normal if and only if $G[F/L]$ is normal in $G[F/K]$ in which case $G[L/K] \cong G[F/K]/G[F/L]$.*

Proof. Theorem 1 says that F/K being algebraic Galois implies it is the splitting field of a set of separable polynomials in $K[x]$ which are also in $L[x]$ so that F can be realized as the splitting field of a set of separable polynomials in $L[x]$. Hence, F/L is Galois.

Now let us suppose that L/K is Galois, and let $x \in L$. Since F/K is algebraic, there is an irreducible polynomial $f \in K[y]$ with x as one of its roots. L/K being Galois means that f splits in $L[y]$ so that all of its roots are in L. Thus, for any $\alpha \in G[F/K]$, since $\alpha(x)$ is also a root of f, we must have $\alpha(x) \in L$. Lemma 2 then implies that $G[F/L]$ is normal. For the reverse direction, let $G[F/L]$ be normal in $G[F/K]$ and $x \in L - K$. Since F/K is Galois, there is an $\alpha \in G[F/K]$ such that $\alpha(x) \neq x$. By Lemma 2, $\alpha\mid_L \in G[L/K]$ so that L/K is indeed Galois.

For the isomorphism, observe that, when L/K is Galois, the mapping $G[F/K] \to G[L/K]$ defined by $\alpha \mapsto \alpha\mid_L$ is a well defined epimorphism with kernel $G[F/L]$. □

The following two lemmas highlight the importance of finite dimensional intermediate fields in any field extension and give us bounds with which the Galois correspondence arises.

Lemma 4. *Let L,M be intermediate fields of the extension F/K with $M \subset L$. If $[L : M]$ is finite, then $[M' : L'] \leq [L : M]$. In particular, if $[F : K]$ is finite, then $|G[F/K]| \leq [F : K]$.*

Proof. See [1] pg. 247. □

Lemma 5. *Let H,J be subgroups of $G[F/K]$ with $H < J$. If $[J : H]$ is finite, then $[H' : J'] \leq [J : H]$.*

Proof. See [1] pg. 248. □

Corollary 6. *If F/K is a finite Galois extension, then every subgroup of $G = G[F/K]$ is Galois closed.*

Proof. Note that G is finite by Lemma 4. For any subgroup H of G, $H < H''$. Applying Lemma 4 and Lemma 5, $|H''| \leq [F : H'] \leq |H|$. □

Corollary 7. *If F/K is a finite dimensional Galois extension, then the inequalities in Lemma 4 and Lemma 5 are equalities.*

Proof. Let $L \subset M$ be intermediate fields and $H < J$ subgroups of $G = G[F/K]$. Theorem 3 implies that $L'' = L$ and $M'' = M$. Applying Lemma 5, $[M : L] = [M'' : L''] \leq [L' : M']$. This together with Lemma 4 gives $[L' : M'] = [M : L]$. A similar proof with the subgroups H and J shows that $[H' : J'] = [J : H]$. □

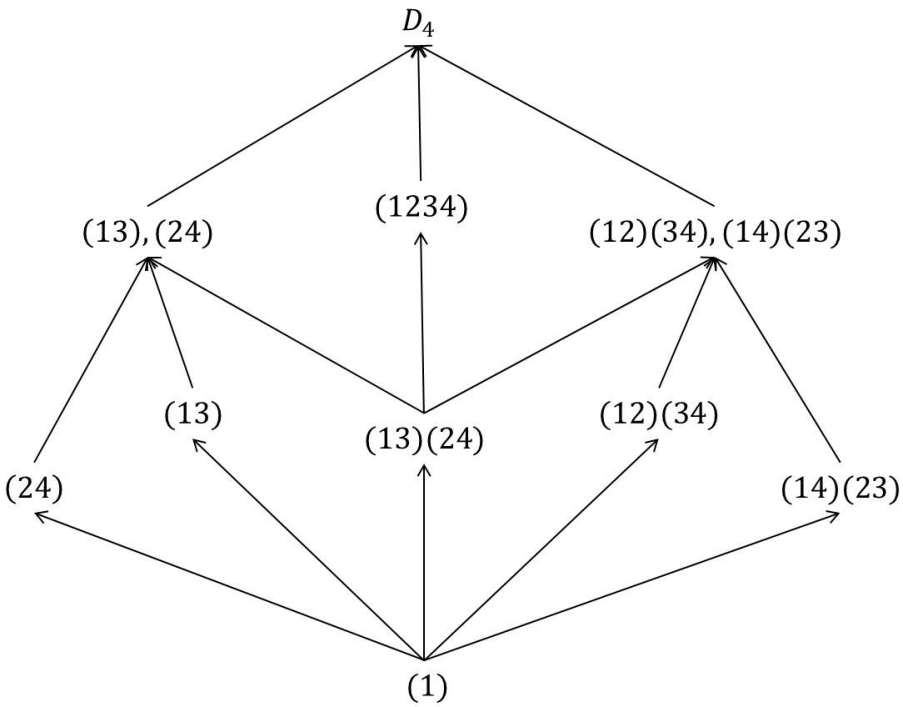
Corollary 8. *If F/K is an algebraic Galois extension, then every finite subgroup of $G[F/K]$ is Galois closed.*

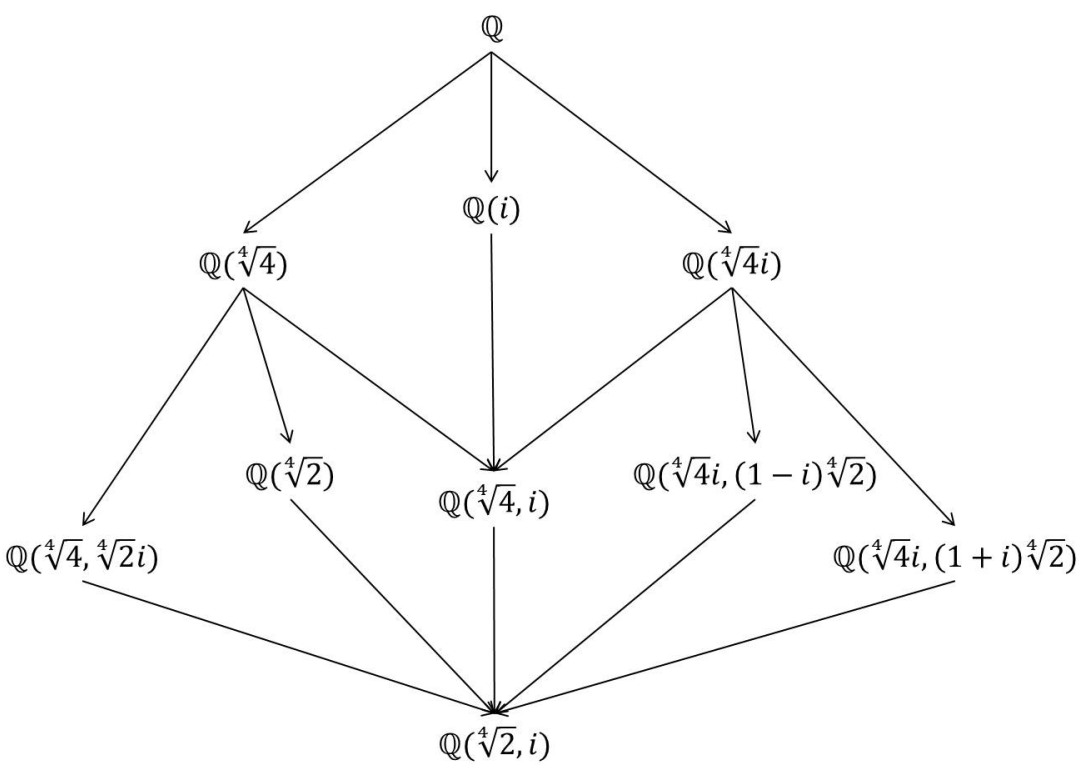
Proof. Let H be a finite subgroup of $G[F/K]$. Then $[F : H^{'}] \leq |H|$ by Lemma 5 so that $[F : H^{'}]$ is finite and hence $|H^{''}| \leq [F : H^{'}]$ is also finite by Lemma 4. Thus, $|H| \leq |H^{''}| \leq [F : H^{'}] \leq |H|$. □

Theorem 9. *(The Galois Correspondence) Let F/K be an algebraic Galois extension with Galois group G. Then there is a bijection between the set of all intermediate fields and all Galois closed subgroups of G.*

Proof. We map each intermediate field L to $G[F/L]$. This mapping is easily seen to be the desired bijection by Theorem 3 and 7. □

Example 10. Consider the splitting field $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$ of the irreducible $x^4 - 2$ over $\mathbb{Q}$. Define $\omega_n = \sqrt[4]{2}i^n$ so that $x^4 - 2 = (x - \omega_1)(x - \omega_2)(x - \omega_3)(x - \omega_4)$ in $\mathbb{Q}\left(\sqrt[4]{2}, i\right)[x]$. We consider the Galois group $G = G\left[\mathbb{Q}\left(\sqrt[4]{2}, i\right)/\mathbb{Q}\right]$ as a subgroup of S_4 acting on $\{1, 2, 3, 4\}$ where each $j = 1, 2, 3, 4$ represents ω_j. It is easy to see that $\left\{1, i, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}, \sqrt[4]{2}i, \sqrt[4]{4}i, \sqrt[4]{8}i\right\}$ forms a basis of the extension in question so that $|G| = 8$ by 7. Each subgroup of order 8 is isomorphic to D_4, and there are precisely three of them by the Sylow Theorems. The three subgroups are $\langle(13), (1234)\rangle$, $\langle(12), (1324)\rangle$, and $\langle(14), (1243)\rangle$. Note that $\omega_1^2 = \omega_3^2$ and $\omega_2^2 = \omega_4^2$. Thus, for a permutation to correspond to a transformation, the just stated algebraic equations must remain satisfied. This implies that (12) and (14) are not permissible so that the Galois group must be $\langle(13), (1234)\rangle$. The subgroup lattice of G and the subspace lattice of $\mathbb{Q}\left(\sqrt[4]{2}, i\right)/\mathbb{Q}$ are given below. For the subgroup lattice, the generators are listed instead of the whole subgroup. Each lattice is in correpondence with the other by the Galois bijection stated in Theorem 9. For example, the subgroup generated by (1234) has fixed field $\mathbb{Q}(i)$ so that their locations match within each respective lattice.





We define the Galois mapping of an extension to be the mapping as in the proof of Theorem 9, namely $\{L : L\, an\, intermediate\, field\, of\, F/K\} \to \{H : H < G[F/K]\}$ defined as $L \mapsto L'$. Regardless if the extension is algebraic or Galois,

if the Galois mapping is well defined, then we call the pair $\{F/K : G[F/K]\}$ a Galois system. If there is a subgroup H of $G[F/K]$ such that every subgroup of H (including H) has a preimage under the Galois mapping, then H is called the minimal Galois group of F/K. In particular, if there is a minimal Galois group H of F/K such that the Galois mapping is a bijection, we will then refer to the Galois mapping as a Galois bijection and the pair $\{F/K : H\}$ as a full Galois system. Thus, as an example of the notation, we may restate the Galois Correspondence (Theorem 9) as follows: If F/K is an algebraic Galois extension with Galois group G, then $\{F/K : G\}$ is a Galois system where the image of the Galois mapping is precisely the collection of all Galois closed subgroups of G. Also, in view of 6, we have the following: If F/K is a finite Galois extension, then $\{F/K : G[F/K]\}$ is a full Galois system. We now present a theorem of Soundararajan that is a partial converse to the Galois correspondence theorem.

Theorem 11. *Let F/K be a field extension with Galois group G and $H < G$. If $\{F/K : H\}$ is a full Galois system, then F/K is algebraic Galois and $H = G_t$, the torsion elements of G.*[1]

Proof. $\{F/K : H\}$ being a full Galois system implies that $G' = H' = K$; hence, F/K is Galois. Let X be a transcendence base of F over K. Then F is an algebraic extension of $K(X)$. For any $k \in F - K(X)$, there is an irreducible polynomial $f \in K[x]$ that is separable and splits over F as, say, $f(x) = (x-x_0)(x-x_1)\cdots(x-x_n) \in F[x]$ with each x_i distinct and $x_0 = k$. Thus, there is an $\alpha \in G$ such that $\alpha(k) = x_j$ for some $j \neq 0$ since F/K is Galois. $F/K(X)$ is therefore an algebraic Galois extension whence $\{F/K(X) : G\}$ and hence $\{F/K(X) : H\}$ is a Galois system by Theorem 9. Furthermore, every Galois closed subgroup of H has a preimage. Thus, to show that F/K is algebraic, i.e., X is empty, it suffices to show that each subgroup of H is Galois closed. This, however, is clear since $\{F/K : H\}$ is a full Galois system.

[1]The theorem, proof of $H = G_t$, and notation are all due to [9].

Let $\alpha \in G[F/K]$ be of finite order with fixed field L. Then F/L is finite by Lemma 5. Furthermore, $\langle\alpha\rangle$ is Galois closed by 8. Thus, $\langle\alpha\rangle < H$ and $\alpha \in H$ so that $G_t \subset H$. For the reverse inclusion, suppose there is a nontrivial $\beta \in H$ of infinite order and let $M = \langle\beta\rangle'$. Let p be prime and define M_p as the set of elements of F that have degrees a power of p over M. Hence, M_p is an intermediate field and $G[M_p/M]$ is trivially normal in $G[F/M] = \langle\beta\rangle$ so that M_p/M is therefore Galois by Theorem 3. Also, there exists a $t \in \mathbb{N}$ such that $G[F/M_p] = \langle\beta^t\rangle$ whence $G[M_p/M] \cong \mathbb{Z}_t$. Thus, since $[F : M(\bigcup_{\substack{q\,prime\\ q\neq p}} M_q)] = [M_p : M]$, $F/M(\bigcup_{\substack{q\,prime\\ q\neq p}} M_q)$ corresponds to a finite subgroup of $\langle\beta\rangle \cong \mathbb{Z}$ which must be the trivial group so that $[F : M(\bigcup_{\substack{q\,prime\\ q\neq p}} M_q)] = [M_p : M] = 1$ and $M = M_p$. Since $F = M(\bigcup_{q\,prime} M_q)$ and p was arbitrary, then $F = M$. This contradicts the nontriviality of β so that we must have $H \subset G_t$ and thus $H = G_t$. □

It is quite worth noting the dependence on finite intermediate extensions in algebraic Galois extensions. Let $\mathcal{F}$ denote the set of all intermediate fields L of an algebraic Galois extension F/K such that L/K is a finite normal extension. Then $F = \bigcup_{L\in\mathcal{F}} L/K$. Hence, F/K is simply a union of finite extensions. Also, the importance of the torsion elements, and hence finite intermediate extensions, can clearly be seen in Theorem 11. Another way of seeing this dependence is by noting that Theorem 1 simply says that a Galois extension is the union of splitting fields of a single separable polynomial where the union runs over all irreducible polynomials that have a root in F. Let $\mathcal{H}$ denote the set of all subgroups of $G = G[F/K]$ that correspond to an intermediate field in $\mathcal{F}$ through the Galois correspondence. $\mathcal{H}$ is thus the set of all Galois closed normal subgroups with finite index. To further exploit this dependence and utilize its usefulness, we develop a topology on the Galois group using $\mathcal{H}$ as a fundamental system of open neighborhoods of the identity. This topology is called the Krull Topology.

Chapter II

The Krull Topology

We first discuss topological groups in a somewhat general sense while keeping in mind the applications to Galois groups. Let G be a group that is also a topological space. G is a topological group if the mappings $(g_1, g_2) \mapsto g_1 g_2$ and $g_1 \mapsto g_1^{-1}$ are continuous with respect to the topology defined on G. Here, $(g_1, g_2) \in G \times G$ where $G \times G$ is given the product topology. We may combine these two continuity conditions into one by forcing the mapping $(g_1, g_2) \mapsto g_1 g_2^{-1}$ to be continuous. Furthermore, this condition is equivalent to the following: given $g_1, g_2 \in G$ and a neighborhood N of $1 \in G$, there exists neighborhoods K_1 and K_2 of 1 such that $(g_1 K)(g_2 K)^{-1} \subset g_1 g_2^{-1} N$. A neighborhood U is called symmetric if $U = U^{-1}$ where U^{-1} is the collection of all inverses of elements in U. A filter base $\mathcal{F}$ on a set X is a nonemtpy collection of subsets that is closed under finite intersections. Additionally, it is required that the empty set is not an element of $\mathcal{F}$. In topological terms, a filter base defines the smallest neighborhoods the topology contains, hence the name filter. We firstly present how to obtain a useful filter base of a topological group and, conversely, how to uniquely define a topology when given a suitable filter base.

Theorem 12. *Let G be a topological group. There exists a fundamental system $\mathcal{H}$ of closed neighborhoods of 1 such that (i) each element of $\mathcal{H}$ is symmetric, (ii) for each $H \in \mathcal{H}$ there is a $K \in \mathcal{H}$ such that $K^2 \subset H$, and (iii) for each $H \in \mathcal{H}$ and $g \in G$, there is a $K \in \mathcal{H}$ such that $K \subset g^{-1} H g$.*

Proof. See [3]. □

We proceed to show how one can uniquely define a topology on a set when given a filter base of that set. Given a filter base Ω on a set X, we define the

associated filter of Ω on X as the set of all subsets of X that contain an element of Ω and will be denoted as $\widetilde{\Omega}$.

Proposition 13. *Let X be a set. Suppose that, for each $x \in X$, there is a filter base Ω_x of X satisfying (i) for each $\omega \in \Omega_x$, $x \in \omega$ and (ii) finite intersections of elements in Ω_x are in Ω_x. Then there exists a unique topology on X such that, for each $x \in X$, $\widetilde{\Omega}_x$ is the collection of all neighborhoods of x and Ω_x is a fundamental system of neighborhoods of x.*

Following the notion of Theorem 13, we prove a similar theorem for topological groups that is somewhat a converse of Theorem 12.

Theorem 14. *Let G be a group and $\mathcal{H}$ a filter base satisfying: (i) each element of $\mathcal{H}$ is symmetric, (ii) for each $H \in \mathcal{H}$, there exists a $K \in \mathcal{H}$ such that $K^2 \subset H$, and (iii) for each $H \in \mathcal{H}$ and $g \in G$, there exists a $K \in \mathcal{H}$ such that $K \subset g^{-1}Hg$. Then there exists a unique topology defined on G such that G is a topological group and $\mathcal{H}$ is a fundamental system of neighborhoods of $1 \in G$.*

Remark. In the following proof, we don't require conditions (i) and (ii) separately; rather, we only require that for each $H \in \mathcal{H}$, there is a $K \in \mathcal{H}$ such that $KK^{-1} \subset H$. However, every topological group has a fundamental system of neighborhoods of $1 \in G$ that are symmetric so that whether we require (i) and (ii) separately or (ii) only, the same topological group will arise.

Proof. Let $H \in \mathcal{H}$. Conditions (i) and (ii) implies there is a $K \in \mathcal{H}$ such that $KK^{-1} = K^2 \subset H$ so that $1 \in H$. It is clear to see that $g\mathcal{H}$ is filter bases since $\mathcal{H}$ is. Also, each $gH \in g\mathcal{H}$ has $g \in gH$ since $1 \in H$. Thus, for each $g \in G$, we have a filter base $g\mathcal{H}$ satisfying the conditions of Theorem 13 so that there is a unique topology such that the collection of all neighborhoods of g is precisely $\widetilde{g\mathcal{H}}$ and $g\mathcal{H}$ is a fundamental system of neighborhoods of g.

We proceed by showing that the mapping $G \times G \to G$ given by $(g_1, g_2) \mapsto g_1 g_2^{-1}$ is continuous in order to conlcude that G is topological group when given the

above topology. Let $g_1, g_2 \in G$ and $g_1 g_2^{-1}\widetilde{N}$ a neighborhood of $g_1 g_2^{-1}$ where $\widetilde{N} \in \widetilde{\mathcal{H}}$. Thus, there is a $N \in \mathcal{H}$ such that $N \subset \widetilde{N}$. By conditions (ii) and (iii), there is a $K \in \mathcal{H}$ such that $K^2 \subset g_2^{-1} N g_2$. Applying condition (i) and the above facts, we see that,

$$(g_1K)(g_2K)^{-1} = g_1KK^{-1}g_2^{-1} = g_1K^2g_2^{-1} \subset g_1(g_2^{-1}Ng_2)g_2^{-1} = g_1g_2^{-1}N \subset g_1g_2^{-1}\widetilde{N}.$$

Hence, the mapping $(g_1, g_2) \mapsto g_1 g_2^{-1}$ is indeed continuous so that G endowed with the specified topology is a topological group. □

Corollary 15. *Let G be a group and $\mathcal{H}$ a filter base of normal subgroups. Then there exists a unique topology such that G is a topological group and $\mathcal{H}$ is a fundamental system of neighborhoods of $1 \in G$.*

Proof. The filter base $\mathcal{H}$ clearly satisfies the conditions of Theorem 14. □

For an algebraic Galois extension F/K, recall that $\mathcal{F}$ is the collection of all finite dimensional intermediate Galois extensions and $\mathcal{H}$ the corresponding normal subgroups of finite index. To see that $\mathcal{H}$ is a filter base, let $M, N \in \mathcal{H}$. Then $(M \bigcap N)'/K$ is a finite dimensional intermediate extension so that $(M \bigcap N)' \in \mathcal{F}$. Since M and N are Galois closed, then it is quite easy to see that $(M \bigcap N)'' = M'' \bigcap N'' = M \bigcap N$ and thus, $M \bigcap N \in \mathcal{H}$.

Definition. Let F/K be an algebraic extension with $\mathcal{H}$ as defined above. The topology defined on $G[F/K]$ in Theorem 14 with filter base $\mathcal{H}$ is called the *Krull Topology.*

Remark. Unless otherwise stated, $G[F/K]$ will be endowed with the Krull topology. Note that if F/K is finite Galois, then the Krull topology coincides with the discrete topology. Let $g \in G[F/K]$. A neighborhood of g is of the form $gG[F/L]$. For any $h \in G[F/K]$, $h \in gG[F/L]$ iff $h\mid_L = g\mid_L$. Thus, two automorphisms of F/K are near in a topological sense if they meet on some intermediate field L

that is finite Galois over K. In particular, for any $H_1, H_2 < G[F/K]$, if $H_1' = H_2'$, then $\overline{H}_1 = \overline{H}_2$.

The remark above gives some insight to the structure uncovered, or, better yet, highlighted by the Krull topology. Before we further explore the Krull topology, we present some useful facts concerning subsets, particularly subgroups, of topological groups.

Proposition 16. *If H is a subgroup of a topological group G, then H is a topological group.*

Proof. The continuity conditions satisfied by G concering the group operation and inversion apply to the subgroup H so that the proposition follows. □

Proposition 17. *Let C be a closed subset of a topological group G. For any $g \in G$, gC, Cg, and C^{-1} are closed in G.*

Proof. If c is a limit point of gC, it is easy to see, then, that $g^{-1}c$ is a limit point of C and hence $g^{-1}c \in C$ and $c = gg^{-1}c \in gC$. Similarly for Cg and C^{-1}. □

Proposition 18. *Let N be an open subset and U any subset of a topological group G. Then UN, NU, and N^{-1} are open in G.*

Proof. Let $un \in UN$. Then there is a neighborhood K of n such that $K \subset N$. Then uK is a neighborhood such that $un \in uK \subset UN$ whence UN is open. Similarly for NU and N^{-1}. □

Proposition 19. *Let $\mathcal{H}$ be the system of neighborhoods of 1 in a topological group G. Then, for any subset A, $\overline{A} = \bigcap_{H \in \mathcal{H}} AH = \bigcap_{H \in \mathcal{H}} HA$.*

Proof. This follows from 18. □

Proposition 20. *If H is a subgroup of a topological group G, then $\overline{H}$ is also a subgroup.*

Proof. This follows from 17. □

Proposition 21. *Every open subgroup H of a topological group G is closed.*

Proof. 18 gives that each coset of H is open so that $H = G - \bigcup_{g \in G-H} gH$ is closed. □

Proposition 22. *Every closed subgroup H of finite index in a topological group G is open.*

Proof. 17 gives that each coset is closed. Since H is of finite index, $\bigcup_{g \in G-H} gH$ can be made into a finite union so that it is also closed and hence, $H = G - \bigcup_{g \in G-H} gH$ is open. □

Proposition 23. *A subgroup H of a topological group G is closed if and only if there exists a closed neighborhood U of 1 such that $H \bigcap U$ is closed. In particular, if H contains a closed neighborhood of 1, then H is closed.*

Proof. The forward direction is trivial so suppose that there is a closed neighborhood U of 1 such that $H \bigcap U$ is closed. There is a symmetric neighborhood V of 1 such that $V^2 \subset U$ by Theorem 12. Let h be a limit point of H and $\{h_i\}_{i \in I}$ a net in H that converges to h. Then h^{-1} is also a limit point of H so that there is a $k \in Vh^{-1} \bigcap H$. Also, there is a $j \in I$ such that for all $i \geq j$, $h_i \in hV$ and hence $kh_i \in Vh^{-1}hV = V^2 \subset U$. Thus, $kh_i \in H \bigcap U$ for all $i \geq j$. Since $H \bigcap U$ is closed, $kh \in H \bigcap U$ whence $h = k^{-1}kh \in H^2 = H$ and H is closed. □

We now continue on to study the topological structure of Galois groups and how that structure relates to the algebraic structure.

Theorem 24. *Let F/K be an algebraic Galois extension with Galois group $G = G[F/K]$. Then $H < G$ is Galois closed if and only if H is closed in the Krull topology. In particular, $\overline{H} = G[F/H']$.*

Proof. Let $H < G$ be Galois closed. Then $H = H'' = \bigcap_{x \in H'} G[F/K(x)]$. For each $x \in H'$, $G[F/K(x)] \in \mathcal{H}$ so that each subgroup in the intersection is open and hence closed in the Krull topology whence H is closed.

Suppose now that H is topologically closed and let $g \in G - \overline{H}$ (the case where $G = \overline{H}$ is trivial). Then there exists an $N \in \mathcal{H}$ such that $gN \bigcap H$ is empty so that $g \notin HN$. Let $h \in H$. If $g\mid_{N'} = h\mid_{N'}$, then $h^{-1}g \in N$ and $g \in HN$. Thus, $g \notin HN$ implies $g\mid_{N'} \neq h\mid_{N'}$ for each $h \in H$ so that there exists an $x \in N' \bigcap H'$ such that $g(x) \neq x$ and hence, $g \notin H''$. Therefore, $g \notin \overline{H}$ implies $g \notin H''$ so that $H'' \subset \overline{H}$. Since H'' is closed by the preceding paragraph, then $H'' = \overline{H} = H$. □

We take a moment to generalize Theorem 24 for possibly nonalgebraic extensions.

Definition. Let F/K be a Galois extensions and $G = G[F/K]$. Define the set $\mathcal{H}^*$ to be the collection of subsets of the form $G - gG[F/K(x)]$ with $g \in G$ and $x \in F$. Then $\mathcal{H}^*$ forms a subbase for a topology on G which we will call the *Galois topology.* [2]

Note that, in general, G is not a topological group when endowed with the Galois topology. However, when the extension is algebraic, we have the following.

Theorem 25. *If F/K is an algebraic Galois extension, then the Galois topology coincides with the Krull topology defined on $G = G[F/K]$.*

Proof. The open subgroups of G under the Galois topology are of the form $\bigcup \left(\bigcap_{i=1}^{n} G[F/K(x_i)] \right) = \bigcup G[F/K(x_1, ..., x_n)]$ so that the filter base $\mathcal{H}$ for the Krull topology is also a filter base for the Galois topology. Hence, by Theorem 14, the theorem follows. □

The usefulness of this topology can be seen in the following generalization of Theorem 24.

[2]This topology, as well as the proof of Theorem 26, is due to Soundararajan. See [10].

Theorem 26. *Let F/K be a Galois extension. A subgroup $H < G[F/K]$ is Galois closed if and only if it is closed in the Galois topology.*

Proof. Let H be Galois closed. Then $H = H'' = \bigcap_{x \in H'} G[F/K(x)]$ which is closed in the Galois topology since $G[F/K(x)] = G - \bigcup_{g \notin G[F/K(x)]} gG[F/K(x)]$.

Now suppose that H is closed in the Galois topology. Let $h \in H''$. We proceed to show that h is in fact a limit point of H via contradiction. That is, suppose that there is a basis element $\bigcap_{i=1}^{n} (G - g_i G[F/K(x_i)])$ that contains h but does not intersect H so that $H \subset \bigcup_{i=1}^{n} g_i G[F/K(x_i)]$. We may assume that no coset in the covering of H can be omitted. Thus, Neumann's Lemma[3] implies that H is covered by finitely many cosets of $\bigcap_{i=1}^{n} G[F/K(x_i)] = G[F/K(x_1, ..., x_n)]$ so that each element of the set $X = \{x_1, ..., x_n\}$ has a finite number of images under H. Let $L = H'(\{h(x) : h \in H, x \in X\})$. Then L/H' is a finite and hence algebraic extension. Furthermore, each element of $L - H'$ is moved by some element of H so that $G[L/H']' = H'$. Thus, the extension is also Galois and the mapping $H \to G[L/H']$ given by restriction is an epimorphism by Theorem 3. Since $h \in H''$, it also restricts to L so that there is an $h^* \in H$ such that $h\mid_L = h^*\mid_L$. Recall that $h \notin \bigcup_{i=1}^{n} g_i G[F/K(x_i)]$ so that $h^* \notin \bigcup_{i=1}^{n} g_i G[F/K(x_i)]$. This contradicts the hypothesis that $H \subset \bigcup_{i=1}^{n} g_i G[F/K(x_i)]$ whence h is indeed a limit point of H and hence $H = H''$. □

Corollary 27. *Let K be a field. All closed subgroups of $Gal(K)$ correspond to all separable algebraic extensions of K. In particular, all closed normal subgroups of $Gal(K)$ correspond to all algebraic Galois extensions of K.*

Proof. This follows immediately from Theorem 3 and Theorem 24. □

Now to analyze the topological structure of Galois groups.

[3] If a group is covered by finitely many cosets, none of which can be omitted, then each coset is of finite index. See [6] for Neumann's proof.

Lemma 28. *Let F/K be an algebraic Galois extension. $G[F/K]$ is isomorphic to a closed subspace of the compact product space $\prod_{L\in\mathcal{F}} G[L/K]$.*

Proof. Define $\varphi : G \to \prod_{L\in\mathcal{F}} G[L/K]$ by $\alpha \mapsto \prod_{L\in\mathcal{F}} \alpha\mid_L$. The proof of Lemma 2 shows that φ is a well defined group homomorphism. Since $F = \bigcup_{L\in\mathcal{F}} L/K$, then the injectivity of φ follows. Denote the projection mapping $\prod_{L\in\mathcal{F}} G[L/K] \to G[L/K]$ by π_L. Since $\pi_L\varphi^{-1}(\{1\}) = G[F/L]$, then $\pi_L\varphi$ is continuous for each $L \in \mathcal{F}$ and hence the continuity of φ follows. Fix $L \in \mathcal{F}$. Define $\mathcal{F}_L = \{M \in \mathcal{F} : M \subset L\}$. Note that $\mathcal{F}_L$ is a finite set. Then $\varphi(G[F/L]) = (\prod_{M\in\mathcal{F}_L} \{1_M\} \times \prod_{M\in\mathcal{F}-\mathcal{F}_L} G[M/K]) \bigcap \varphi(G)$ which is open in $\varphi(G)$. Hence, $G \cong \varphi(G)$.

It is easy to see that $\varphi(G) = \{(\alpha_L)_{L\in\mathcal{F}} \in \prod_{L\in\mathcal{F}} G[L/K] : \pi_{L_2}(\alpha_L)\mid_{L_1} = \pi_{L_1}(\alpha_L)$ $\forall L_1 \subset L_2\} = \bigcap_{L_1\subset L_2} \{(\alpha_L)_{L\in\mathcal{F}} \in \prod_{L\in\mathcal{F}} G[L/K] : \pi_{L_2}(\alpha_L)\mid_{L_1} = \pi_{L_1}(\alpha_L)\}$. Since all the projection mappings are continuous and each $G[L/K]$ is Hausdorff, then $\varphi(G)$ is closed in the compact product space $\prod_{L\in\mathcal{F}} G[L/K]$. □

Theorem 29. *If G is the Galois group of an algebraic Galois extension F/K, then G is a totally disconnected compact topological group.*

Proof. Observe that $\bigcap_{L\in\mathcal{F}} G[F/L] = \{1\}$ since $F = \bigcup_{L\in\mathcal{F}} L/K$ and hence G is totally disconnected. Lemma 28 implies that G is compact. □

Proposition 30. *Let F/K be an algebraic Galois extension with Galois group G. Then the open subgroups of G are precisely the groups $G[F/L]$ where L/K is a finite intermediate extension; furthermore, the closed subgroups are precisely the intersections of open subgroups.*

Remark. The collection of all finite intermediate extensions is quite different from $\mathcal{F}$, the collection of all finite Galois intermediate extensions.

Proof. Let $\mathcal{H}$ be defined as usual and let $G[F/L]$ be a subgroup with L/K a finite intermediate extension. Then there is a finite Galois extension $\widetilde{L}$ that contains L. Thus, $G[F/\widetilde{L}] < G[F/L]$ and $G[F/L] = \bigcup_{g\in G[F/L]} gG[F/\widetilde{L}]$ is open by 18.

Let $H < G$ be an open subgroup. Then there is a $\widetilde{H} \in \mathcal{H}$ with $\widetilde{H} < H$. Let $\widetilde{L}$ be the fixed field of $\widetilde{H}$ and consider the natural epimorphism $\pi : G \to G/G[F/\widetilde{L}]$. Then $\pi(H) = G[\widetilde{L}/L]$ for some finite intermediate field L of $\widetilde{L}/K$ by 8. Thus, $H < G[F/L]$. Since H is closed by 21 and $H^{'} = L$, then Theorem 9 implies that $H = G[F/L]$.

The intersection of open subgroups is closed by 21. For any closed subgroup H, $H = \bigcap_{M \in \mathcal{H}} HM$ by 19 which is an intersection of open subgroups by 18. $\square$

Chapter III

Profinite Groups: The Structure of Galois groups

Let I be a directed set and Top the category of topological spaces. An inverse system $(T_i, f_{ij})_{i,j\in I}$ is a collection of objects T_i in Top and continuous functions $f_{ij} : T_j \to T_i$ for $i \leq j$ such that f_{ii} is the identity map on T_i and $f_{ik} = f_{ij}f_{jk}$ whenever $i \leq j \leq k$. An inverse limit of the inverse system $(T_i, f_{ij})_{i,j\in I}$ is an object $T \in$ Top together with continuous functions $\pi_i : T \to T_i$ called projections satisfying $\pi_i = f_{ij}\pi_j$ whenever $i \leq j$. Additionally, T is determined according to the following universal property: for any other object $D \in$ Top together with continuous functions $\psi_i : D \to T_i$ satisfying $\psi_i = f_{ij}\psi_j$ whenever $i \leq j$, there exists a unique continuous function $\varphi : D \to T$ such that $\psi_i = \pi_i\varphi$ for each $i \in I$. Firstly, we address the existence and uniqueness of inverse limits in Top.

Theorem 31. *Given any inverse system $(T_i, f_{ij})_{i,j\in I}$ in* Top*, there exists an inverse limit $(T, \varphi_i)_{i\in I}$. Furthermore, for any other inverse limit $(D, \psi_i)_{i\in I}$ of $(T_i, f_{ij})_{ij\in I}$, there exists a homeomorphism $\Phi : D \to T$ such that $\psi_i = \varphi_i\Phi$ for each $i \in I$.*

Proof. Let $T = \{t \in \prod_{i\in I} T_i \ : \ \pi_i(t) = f_{ij}\pi_j(t)\ \forall i, j \in I,\ i \leq j\}$ where π_i denotes the projection $\prod_{j\in I} T_j \to T_i$ and define the continuous mappings $\varphi_i = \pi_i\,|_T$ for $i \in I$. We show that $(T, \varphi_i)_{i\in I}$ is an inverse limit of $(T_i, f_{ij})_{i,j\in I}$.

By construction, $\varphi_i = f_{ij}\varphi_j$ whenever $i \leq j$. Let $(D, \psi_i)_{i\in I}$ be an inverse limit of $(T_i, f_{ij})_{i,j\in I}$. Define the map $\tilde{\phi} : D \to \prod_{i\in I} T_i$ by $d \mapsto \{\psi_i(d)\}_{i\in I}$. Clearly $\psi_i = \pi_i\tilde{\phi}$ for each $i \in I$ so that $\tilde{\phi}$ is continuous. Furthermore, for any $i, j \in I$ with $i \leq j$ and $d \in D$, $\pi_i(\tilde{\phi}(d)) = \psi_i(d) = f_{ij}\psi_j(d) = f_{ij}\pi_j(\tilde{\phi}(d))$ whence $\mathrm{Im}\tilde{\phi} \subset T$ which enables us to define the continuous mapping $\phi : D \to T$ by $d \mapsto \tilde{\phi}(d)$. Note that ϕ is unique by construction. We now see that $\psi_i = \varphi_i\phi$ for each $i \in I$ so that $(T, \varphi_i)_{i\in I}$ is indeed an inverse limit of $(T_i, f_{ij})_{i,j\in I}$.

We now proceed to the uniqueness of an inverse limit. Let $(D, \psi_i)_{i\in I}$ be any other inverse limit of $(T_i, f_{ij})_{i,j\in I}$. Then there exists unique continuous maps $\Phi : D \to T$ and $\Psi : T \to D$ such that $\psi_i = \varphi_i\Phi$ and $\varphi_i = \psi_i\Psi$. Thus, $\varphi_i = \varphi_i\Phi\Psi$ and $\psi_i = \psi_i\Psi\Phi$. Since Φ and Ψ are unique, then $\Phi\Psi = id\ |_T$ and $\Psi\Phi = id\ |_D$ whence Φ is a homeomorphism. □

Thus, given any inverse system $(T_i, f_{ij})_{i,j\in I}$ in Top, we may define the inverse limit as in the proof of Theorem 31 which is unique up to homeomorphism. We will denote the inverse limit as $\underleftarrow{lim} T_i$ together with the projection maps $\varphi_i : \underleftarrow{lim} T_j \to T_i$. Topologically, we let $\prod_{i\in I} T_i$ have the product topology and view $\underleftarrow{lim} T_i$ as a subspace of $\prod_{i\in I} T_i$. We now concern ourselves with some topological properties that the inverse limit inherits from the elements of the inverse system. If each T_i is totally disconnected, then $\underleftarrow{lim} T_i$ is totally disconnected. This follows from topological spaces maintaining totally disconnectedness through products and subspaces. We also have the following.

Theorem 32. *If $(T_i, f_{ij})_{i,j\in I}$ is an inverse system in* Top *such that each T_i is Hausdorff and compact, then $\underleftarrow{lim} T_i$ is compact.*

Proof. By the Theorem of Tychonoff, $\prod_{i\in I} T_i$ is compact. Thus, it suffices to show that $\underleftarrow{lim} T_i$ is closed in $\prod_{i\in I} T_i$. Recall that $\underleftarrow{lim} T_i = \{t \in \prod_{i\in I} T_i : \pi_i(t) = f_{ij}\pi_j(t)\ \forall i, j \in I, i \leq j\}$ so that $\underleftarrow{lim} T_i = \bigcap_{j\in I}\{t \in \prod_{i\in I} T_i : \pi_i(t) = f_{ij}\pi_j(t)\ \forall i \leq j\}$, the intersection indexing through all $j \in I$. Thus, $\underleftarrow{lim} T_i$ is closed since each π_i and $f_{ij}\pi_j$ is continuous and each T_i is Hausdorff. □

Thus, if $(T_i, f_{ij})_{i,j\in I}$ is an inverse system in Top such that each T_i is Hausdorff and compact, then $\underleftarrow{lim} T_i$ is Hausdorff and compact. In particular, if each T_i is totally disconnected and compact, then $\underleftarrow{lim} T_i$ is totally disconnected and compact.

Since we are concerned with topological groups, we prove one more important fact about inverse limits in Top concerned with topological groups. When talking about topological groups, the term homomorphism (resp. isomorphism) will refer

to a mapping that is a group homomorphism (resp. group isomorphism) that is also continuous. We say that an inverse system $(T_i, f_{ij})_{i,j\in I}$ in Top is an inverse system of topological groups if each T_i is a topological group and each f_{ij} is a homomorphism.

Theorem 33. *If $(T_i, f_{ij})_{i,j\in I}$ is an inverse system of topological groups, then $\varprojlim T_i$ is a topological group. Furthermore, $\varprojlim T_i$ is uniquely determined up to isomorphism.*

Proof. Since $\prod_{i\in I} T_i$ is a topological group, then it suffices to show that $\varprojlim T_i$ is a subgroup of $\prod_{i\in I} T_i$. Since $\varprojlim T_i = \{t \in \prod_{i\in I} T_i \ : \ \pi_i(t) = f_{ij}\pi_j(t)\ \forall i, j \in I,\ i \leq j\}$ with each π_i and f_{ij} homomorphisms, then $\varprojlim T_i$ contains the identity and is closed under the group operation and taking inverses.

The fact that $\varprojlim T_i$ is uniquely determined up to isomorphism follows immediately from Theorem 31. □

Lemma 34. *If $(T_i, f_{ij})_{i,j\in I}$ is an inverse system of nonempty compact Hausdorff spaces, then $\varprojlim T_i$ is nonempty.*

Proof. We write $\varprojlim T_i = \bigcap_{j\in I} X_j$ as in Theorem 32 where $X_j = \{t \in \prod_{i\in I} T_i \ : \ \pi_i(t) = f_{ij}\pi_j(t) \forall i \leq j\}$ is a closed set. Each X_j can be considered nonempty by the Axiom of Choice. For each $i, j \in I$ with $i \leq j$, $X_j \subset X_i$. Thus, the collection $\{X_i \ : \ i \in I\}$ of closed sets has the finite intersection property whence the compactness of $\prod_{i\in I} T_i$ implies that $\bigcap_{j\in I} X_j$ is nonempty. □

Definition. A group G is *profinite* if $G \cong \varprojlim G_i$ with each G_i a finite group given the discrete topology.

We immediately see that G is a compact totally disconnected topological group by Theorem 32. There are many structural similarities between profinite groups and Galois groups of algebraic Galois systems. They, in fact, give the same class of groups. We will prove this shortly. That being said, we will examine part of

the structure of profinite groups the analog of which we have yet to describe for Galois groups of algebraic Galois extensions.

Firstly, we present a theorem of van Dantzig, the proof of which is outlined in the appendix.

Theorem 35. *(van Dantzig's Theorem) Let G be a totally disconnected locally compact topological group. Then the collection of all compact open subgroups of G forms a basis of neighborhoods of* 1.

We are now ready to give a characterization of profinite groups.

Theorem 36. *If G is a compact totally disconnected topological group, then G is profinite.*

Proof. By van Dantzig's Theorem, the collection $\mathcal{H}^*$ of all open subgroups forms a basis of compact open neighborhoods of 1. Elements of $\mathcal{H}^*$ have finite index by compactness so that for any $H \in \mathcal{H}^*$, $U_H = \bigcap_{g \in G} gHg^{-1}$ is open. Thus, the collection $\mathcal{H} = \{U_H : H \in \mathcal{H}^*\}$ forms a basis of normal compact open subgroups. Define $\varphi : G \to \prod_{H \in \mathcal{H}} G/H$ by $g \mapsto (gH)_{H \in \mathcal{H}}$. The details in the proof of Lemma 28 apply here to show that $G \cong \varphi(G) = \varprojlim_{H \in \mathcal{H}} G/H$. □

Corollary 37. *If H is a closed subgroup of a profinite group, then H is profinite.*

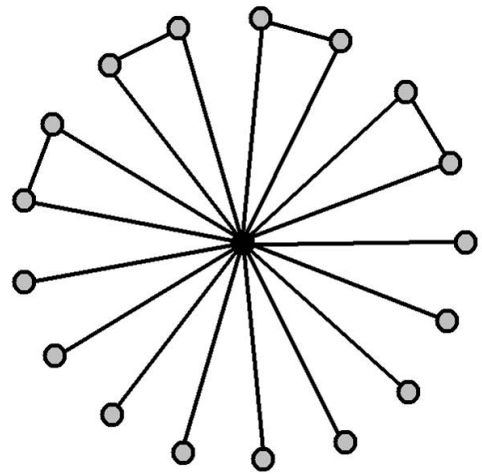
Proof. H is clearly compact and totally disconnected. Thus, the result then follows from 16 and 36. □

Proposition 38. *If F/K is an algebraic Galois extension, then $G[F/K]$ is profinite.*

Proof. The proof of Lemma 28 gives $G[F/K] \cong \varphi(G[F/K])$ where $\varphi : G[F/K] \to \prod_{L \in \mathcal{F}} G[L/K]$ is defined by $\alpha \mapsto (\alpha\ |_L)_{L \in \mathcal{F}}$. Furthermore, the same proof shows clearly that $\varphi(G[F/K]) = \varprojlim_{L \in \mathcal{F}} G[L/K]$ so that $G[F/K]$ is indeed profinite. □

Note. It is important to note that it is necessary for F/K to be both algebraic and Galois. It's easy to consider why F/K being only algebraic would not suffice. For an extension that is Galois but not algebraic, consider $\mathbb{Q}(x_1, x_2)/\mathbb{Q}$ with x_1 and x_2 indeterminates. Under the Krull topology, since there are no intermediate fields that are finite over $\mathbb{Q}$ except $\mathbb{Q}$ itself, $G[\mathbb{Q}(x_1, x_2)/\mathbb{Q}]$ is an infinite discrete group so that it is not compact. Consequently, $G[\mathbb{Q}(x_1, x_2), \mathbb{Q}]$ is not profinite.

Example 39. Consider the extension $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{3}, \zeta_3\right)/\mathbb{Q}$ as a splitting field of $(x^3 - 2)(x^3 - 3)$ where ζ_3 is a third root of unity different from 1. It is easy to check that the Galois groups of $\mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)/\mathbb{Q}$ and $\mathbb{Q}\left(\sqrt[3]{3}, \zeta_3\right)/\mathbb{Q}$, corresponding to the splitting fields of $x^3 - 2$ and $x^3 - 3$ respectiviely, are both S_3. Lemma 28 implies that the Galois group $G = G\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{3}, \zeta_3\right)/\mathbb{Q}\right]$ is a subgroup of $S_3 \times S_3$. It is not the whole space, however, since ζ_3 is in *both* splitting fields. 38 implies that the permutations in $S_3 \times S_3$ that are admissible are the ones which projections onto $\mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$ and $\mathbb{Q}\left(\sqrt[3]{3}, \zeta_3\right)$ are compatible. Upon construction of the Galois groups of the intermediate splitting fields, one sees that the odd permutations transpose ζ_3 and ζ_3^2 while even permutations leave elements in common with $\mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$ and $\mathbb{Q}\left(\sqrt[3]{3}, \zeta_3\right)$ unchanged. Thus, G is the nonabelian subgroup of $S_3 \times S_3$ of order 18 defined by pairing even permutations with even permutations and odd permutations with odd permutations. There are 9 elements of order 2 and 8 elements of order 3. The cylce graph is shown below.



Theorem 40. *Let G be a topological group. Then the following are equivalent.*

(1) G is the Galois group of some algebraic Galois extension.

(2) G is totally disconnected and compact.

(3) G is profinite.

(4) There exists a set of normal compact open subgroups $\{G_i\}_{i\in I}$ that forms a basis of neighborhoods of $1 \in G$ such that $\bigcap_{i\in I} G_i = \{1\}$.

Proof. (1) $\Rightarrow$ (2) is Theorem 29. (1) $\Rightarrow$ (3) is 38. (1) $\Rightarrow$ (4) follows from (2) and van Dantzig's Theorem (Theorem 35). (4) $\Rightarrow$ (2) and (3) $\Rightarrow$ (2) are trivial. We conclude the proof by showing (2) $\Rightarrow$ (1)[4].

Let G be a totally disconnected compact topological group. Define $\mathcal{H}$ as in the proof of 36 and let $\mathcal{L} = \{gH : g \in G, H \in \mathcal{H}\}$. Let f be a field. We consider the elements of $\mathcal{L}$ as indeterminates and define $F = f(\mathcal{L})$, the set of all rational functions of the indeterminates in $\mathcal{L}$ with coefficients in f. G acts naturally on $\mathcal{L}$ by $g(g'H) = gg'H$ and hence on F as $f - automorphisms$. Let $K = \{x \in F : g(x) = (x)\ \forall g \in G\}$.

We show that F/K is algebraic. Let $x \in F$. Denote the set $\{g \in G : gx = x\}$ as G_x. If the indeterminates that appear in the rational expression of x are $\left\{g_{ij}H_i : i = 1, ..., n, j = 1, ..., m\right\}$, then the normality of each H_i implies that $\bigcap_i H_i \subset$

[4]The proof of (2) $\Rightarrow$ (1) is due to [7].

G_x so that G_x is open. By compactness of G, G_x is of finite index whence the orbit of x under the action of G is finite, say $\{x, x_2, ..., x_r\}$. Then $(y - x)(y - x_2) \cdots (y - x_r) \in K[y]$ so that x is algebraic over K.

Since the polynomial in the preceding paragraph has distinct roots, then x is separable over K so that F/K is a separable extension. For each $x \in F$, denote the orbit of x under the action of G as Ox. Since the polynomial for x discussed in the previous paragraph is split, then $F = \bigcup_{x \in F} K(Ox)/K$ is a normal extension. Hence, F/K is an algebraic Galois extension.

It remains to be shown that $G = G[F/K]$. Since $G' = G[F/K]' = K$, then it suffices to show that G is closed in $G[F/K]$ by Theorem 9. Let H be an open normal subgroup of $G[F/K]$ and $L = H'$. Since H is of finite index, then F/L is finite by Lemma 5. Hence, since F/L is algebraic, $L = K(f_1, ..., f_s)$ for some $f_1, ..., f_s \in F$. The preceding paragraphs show that each G_{f_i} is closed. Thus, since $\bigcap_i G_{f_i} \subset G \bigcap H$, $G \bigcap H$ is closed by 23. Hence, G is closed agian by 23 which completes the proof. □

Definition. Let G be a profinite group. A subset X of G will be said to generate G if (i) $\overline{(X)} = G$ where (X) is the subgroup generated by the set X and (ii) every open subgroup of G intersects X at all but a finite number of points.

We present one theorem regarding generating sets that we use for analyzing when a Galois group is metrizable.

Theorem 41. *Let G be a profinite group and X a generating set. Then $|X| \leq \aleph_0$ if and only if G admits a countable descending chain of open normal subgroups $G = G_0 > G_1 > \cdots$ such that $\bigcap_{n \in \mathbb{N}} G_n = \{1\}$.*

Proof. See [8]. □

Definition. Let G be a topological group. G is said to be metrizable if there exists a countable fundamental system of neighborhoods $\{U_n\}_{n\in\mathbb{N}}$, of 1 satisfying the conditions of Theorem 14 such that $\bigcap_{n\in\mathbb{N}} U_n = \{1\}$.

It is well known that this definition is equivalent to the existence of an invariant metric for G such that the metric space topology corresponds with the original topology. For a proof of this, see [3].

Theorem 42. *Let F/K be an algebraic Galois extension with Galois group G. Then G is metrizable if and only if $\mathcal{H}$ is countable. In particular, G is metrizable if and only if it is a splitting field of a countable set of polynomials.*

Proof. Follows immediately from Theorem 1 and Theorem 41. □

We now move on to some group structure. We have seen how one can completely describe an algebraic Galois extension F/K by describing its finite Galois extensions, $\mathcal{F}$, which corresponds to finite Galois quotients of the Galois group, $\{G[L/K] : L \in \mathcal{F}\}$. One can then obtain F from $\mathcal{F}$ by $F = \bigcup_{L\in\mathcal{F}} K(L)$. Likewise, the Galois group can be obtained from $G[F/K]/\mathcal{H}$ by $G[F/K] = \varprojlim_{L\in\mathcal{F}} G[L/K]$. It thus serves reason to examine the finite groups in the inverse limit that defines $G[F/K]$. Since the primes in the order of a finite group play a large role in its structure, one needs to redefine the order $G[F/K]$ in such a way that the primes that divide the orders of the finite Galois quotients of $G[F/K]$ can be explicitly found within the order of $G[F/K]$. Thus enters the so called supernatural numbers.

Definition. A *supernatural number* is a formal product of the form $n = \prod_{p\,prime} p^{n(p)}$ where $n(p)$ is either a non-negative integer or ∞. If n and m are two supernatural numbers, then $n \mid m$ if $n(p) \leq m(p)$ for each prime p. For any family of natural numbers $\{n_i\}_{i\in I}$, we define the following:

- product: $\prod_{i\in I} n_i = \prod_{p\,prime} p^{n(p)}$ where $n(p) = \sum_{i\in I} n_i(p)$;

- greatest common divisor: $gcd(n_i)_{i\in I} = \prod_{p\,prime} p^{n(p)}$ where $n(p) = min\,\{n_i(p)\}_{i\in I}$;
- least common multiple: $lcm(n_i)_{i\in I} = \prod_{p\,prime} p^{n(p)}$ where $n(p) = max\,\{n_i(p)\}_{i\in I}$.

Note. Let p be a prime. We give a clearer definition of the minimum and maximum operations used above. Define the set J by $\left\{n_j(p)\right\}_{j\in J} = \{n_i(p) \,:\, i \in I,\, n_i(p) < \infty\}$. If J is nonempty, then $min\,\{n_i(p)\}_{i\in I} = min\left\{n_j(p)\right\}_{j\in J}$ which always exists and is a non-negative integer. If J is empty, then $min\,\{n_i(p)\}_{i\in I} = \infty$. Likewise, if $I - J$ is nonempty, then $max\,\{n_i(p)\}_{i\in I} = \infty$. If $J = I$, then $max\,\{n_i(p)\}_{i\in I}$ either exists and is a non-negative integer or does not exist in which case we define it to be ∞.

Let G be the Galois group of an algebraic Galois extension F/K. For any closed subgroup $H < G$, we redefine the index of H in G as the supernatural number $[G : H] = lcm\,\{[G[F/K]/G[F/L] : HG[F/L]/G[F/L]] \,:\, L \in \mathcal{F}\}$. This is well defined because $HG[F/L]$ is a subgroup of $G[F/K]$ by the normality of $G[F/L]$ and $G[F/K]/G[F/L] \cong G[L/K]$ is a finite group. In particular, we identify the order of G as $|G| = [G : 1] = lcm\,\{|G[L/K]| \,:\, L \in \mathcal{F}\}$. For convenience, we consider G a profinite group. A pro-p group, p prime, is a profinite group in which the inverse system consists of p-groups. Recall that a Sylow p-subgroup of a finite group G is a subgroup H that has order a power of p and $|G/H|$ is not divisible by p. Likewise, for a profinite group G, a Sylow p-subgroup is a closed subgroup H such that H is a pro-p group and $[G : H]$ is not divisble by p. The intention here is to present a structure theorem for profinite groups analogous to the Sylow theorems for finite groups. We thus have the following theorem.

Theorem 43. *(Sylow Theorem) Let $(G_i, \varphi_{ij})_{i,j\in I}$ be a surjective inverse system of finite groups and p a prime. Let G be the profinite group $\varprojlim G_i$. Then,*

(1) G contains a Sylow p-subgroup;

(2) Any pro-p subgroup is contained in a Sylow p-subgroup of G;

(3) Any two Sylow p-subgroups of G are conjugate.

Proof. (1) Define $\mathcal{P}_i$ as the set of all Sylow p-subgroups of G_i for each $i \in I$. Note that each $\mathcal{P}_i$ is nonempty. Let $i, j \in I$ with $i \leq j$. Since $G_i \cong G_j/ker\,\varphi_{ij}$ and each Sylow p-subgroup of $G_j/ker\,\varphi_{ij}$ is of the form $Pker\,\varphi_{ij}/ker\,\varphi_{ij}$ with P a Sylow p-subgroup of G_j, then, for each $P \in \mathcal{P}_j$, $\varphi_{ij}(P) \in \mathcal{P}_i$. Thus, we may define the mapping $\widetilde{\varphi}_{ij} : \mathcal{P}_j \to \mathcal{P}_i$ by $P \mapsto \varphi_{ij}(P)$. Hence, $(\mathcal{P}_i, \widetilde{\varphi}_{ij})_{i,j\in I}$ is an inverse system of nonempty finite sets so that $\underleftarrow{lim}\mathcal{P}_i$ is nonempty by Lemma 34. Let $(P_i)_{i\in I} \in \underleftarrow{lim}\mathcal{P}_i$. Then $(P_i, \varphi_{ij})_{i,j\in I}$ is an inverse system of finite groups so that $\underleftarrow{lim}P_i$ is easily seen to be a Sylow p-subgroup of G.

(2) Let H be a pro-p subgroup of G. Then $\pi_i(H)$ is a p-subgroup of G_i for each $i \in I$. Define $\mathcal{P}_i$ to be the nonempty collection of Sylow p-subgroups of G_i containing $\pi_i(H)$. Construct $P = \underleftarrow{lim}P_i$ where $(P_i)_{i\in I} \in \underleftarrow{lim}\mathcal{P}_i$ as in previous paragraph so that P is a Sylow p-subgroup of G containing H.

(3) Let H and K be two Sylow p-subgroups of G. Define $C_i = \{c \in G : c\pi_i(H)c^{-1}$
$= \pi_i(K)\}$. Since $\pi_i(H)$ and $\pi_i(K)$ are Sylow p-subgroups of G_i for each $i \in I$, then each C_i is nonempty. Let $i, j \in I$ with $i \leq j$. Also, let $c_i \in \varphi_{ij}(C_j)$ and $c_j \in C_j$ be such that $\varphi_{ij}(c_j) = c_i$. Then $c_i\pi_i(H)c_i^{-1} = \varphi_{ij}(c_j\pi_j(H)c_j^{-1}) = \varphi_{ij}\pi_j(K) = \pi_i(H)$ so that $\varphi_{ij}(C_j) \subset C_i$ whence $(C_i, \varphi_{ij})_{i,j\in I}$ is an inverse system of nonempty finite sets. Lemma 34 implies that $\underleftarrow{lim}C_i$ is nonempty so let $c \in \underleftarrow{lim}C_i$. Then $\pi_i(cHc^{-1}) = \pi_i(c)\pi_i(H)\pi_i(c)^{-1} = \pi_i(K)$ for each $i \in I$ so that $cHc^{-1} = K$. □

As is immediately clear from the Sylow theorems, profinite groups made up of finite $p-groups$ play an important role in the overall structure of Galois groups. Thus, we present the following example.

Example 44. Let p and q be distinct primes. For each $n \in \mathbb{N}$, denote $\mathbb{F}_{q^{p^n}}$ as the unique extension of $\mathbb{F}_q$ as a splitting field of $x^{q^{p^n}} - x$. The Galois group of each intermediate extension $\mathbb{F}_{q^{p^n}}/\mathbb{F}_q$ is therefore the cyclic group $\mathbb{Z}/p^n\mathbb{Z}$. Therefore, Lemma 28 implies that $G = G\left[\bigcup_{n\in\mathbb{N}} \mathbb{F}_{q^{p^n}}/\mathbb{F}_q\right]$ is a subgroup of $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$. The precise subspace is found by analyzing the compatibility of the projection mappings

$\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ for all $m < n$. Thus, any transformation in $\mathbb{Z}/p^n\mathbb{Z}$ that permutes elements that are roots of $x^{q^{p^m}} - x$ must be compatible with the corresponding element in $\mathbb{Z}/p^m\mathbb{Z}$ under the projection mapping. Algebraically, this implies that $G = \bigcap_{n\in\mathbb{N}} \left\{ (\alpha_i) \in \prod_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z} \,:\, \alpha_m \equiv \alpha_n \, mod \, p^m \, \forall \, m < n \right\}$. Thus, $G = \mathbb{Z}_p$, the $p-adic$ integers.

Thus, we see that the structure of Galois groups of infinite Galois extensions depend directly on their finite quotients as is explicitly stated in 38. In fact, infinite Galois groups share much of the same topological and group structure as finite groups as seen in Theorem 29 and Theorem 43.

Chapter IV

A Discussion of Galois Theories Present in Modern Mathematics [5]

One explicit application of Galois theory is in algebraic number theory where the fundamental object of research is number fields which are finite algebraic extensions of $\mathbb{Q}$. These extensions are not always Galois, but they of course are not far away from being splitting fields. Often enough, one works explicitly with Galois number fields. For example, a topic of great importance in algebraic number theory is class field theory which is the study of finite Abelian extensions of number fields. An Abelian extension is an algebraic Galois extension such that the corresponding Galois group is Abelian. An example of such is the algebraic function field of elliptic curves over finite fields. Another example in algebraic number theory is when one considers unique factorization in rings of integral elements of a number field. It is known that rings of integers are Dedekind domains, that is, integral domains such that every proper ideal has a unique factorization into prime ideals. However, rings of integers are not in general unique factorization domains. Regardless, Galois theory aids in calculating the prime ideal factorization as follows: when an extension of number fields F/K is Galois, the Galois group $G[F/K]$ acts transitively on the prime ideals of $\mathcal{O}_F$, the ring of integral elements in F, that are generated by prime ideals in $\mathcal{O}_K$, the ring of integral elements in K, and therefore gives insight into what is called the ramification of the extension which corresponds to the multiplicity of the prime ideals in the factorization of any such ideal. For local fields, one considers extensions of the $p-adic$ numbers in which case ramification quantifies how far an automorphism in $G[F/K]$ sends an integral element under the $p-adic$ metric.

An analog of Galois theory can be found in algebraic topology, namely in certain considerations of covering spaces. Let X be a locally path connected

[5] For a reference to algebraic number theory topics, see [5]. For a reference to covering spaces, see [2]. For a reference to locally compact groups, see [4].

topological space and $\pi_1(X)$ its fundamental group. Then there is a bijective correspondence between the conjugacy classes[6] of $\pi_1(X)$ and all connected covers. Given a covering $p : C \to X$, a homeomorphism φ of C is a deck transformation if $p\varphi = p$. The set of deck transformations, denoted $Aut(p)$, forms a group and is connected to the Galois theory of covering spaces as follows. A covering is called Galois (or regular) if the corresponding subgroup of $\pi_1(X)$ is normal in which case the quotient group is isomorphic to the group of deck transformations of the given cover. Furthermore, a covering can be seen to be Galois if its group of deck transformations acts transitively on some fiber in which case it acts transitively on all fibers of the covering. In this case, if $Aut(p)$ is finite, then the order of $Aut(p)$ is the order of each fiber. The universal cover $\widetilde{X}$ of X is a simply connected covering of X.[7] $\widetilde{X}$ can be classified in a number of ways, one of which is the covering corresponding to the trivial subgroup of $\pi_1(X)$. Obviously the group of deck transformations of the covering $\widetilde{X} \to X$ is isomorphic to $\pi_1(X)$. For example, the fundamental group of S^1 can be calculated by considering the deck transformations of the universal covering $p : \mathbb{R} \to S^1$ defined by $r \mapsto e^{2\pi i r}$ which is clearly $\mathbb{Z}$.

Let G be any compact group and denote the connected component of $1 \in G$ by G^0. Then since $\overline{G^0}$ is also connected and $gG^0g^{-1} \cong G^0$ for each $g \in G$, G^0 is a closed normal subgroup of G and G/G^0 is a totally disconnected group. It is easy to see that both G^0 and G/G^0 are also compact. Thus, 36 says that G/G^0 is profinite. Further, we have a short exact sequence $0 \to G^0 \to G \to G/G^0 \to 0$. G may therefore be viewed as an extension of a profinite group G/G^0 by a connected compact group G^0. Conversely, given a short exact sequence $0 \to K \to G \to H \to 0$ where K is connected and H is totally disconnected, then $K \cong G^0$ and $H \cong G/G^0$. The Gleason-Yamabe Theorem essentially says that for any compact

[6]The bijection concerns conjugacy classes instead of subgroups due to the dependence of base point.

[7]Letting X be semilocally simply connected is one way to ensure existence of the universal cover.

normal subgroup N of G^0, G^0/N is a Lie group. In particular, if G, or just G^0 is also Hausdorff, then G^0 is an inverse limit of Lie groups; this applies especially to G/G^0, but these Lie groups are necessarily finite so that G/G^0 is indeed profinite as already stated. This justifies studying connected compact groups and profinite groups in the more general study of compact groups. One may even extend this to locally compact groups. In fact, if a group G is locally compact, Hausdorff, first countable, and finite dimensional with respect to embeddings of open subsets of $\mathbb{R}^n$ or some generalization thereof, then G is locally isomorphic to the direct product of a Lie group and a profinite group as in the compact case.

References

[1] Hungerford, Thomas W., *Algebra.* New York: Springer, 1974.

[2] Hatcher, Allen., *Algebraic Topology.* Allen Hatcher, 2001.

[3] Husain, T., *Introduction to Topological Groups.* Philadelphia and London: W. B. Saunders Company, 1966.

[4] Kaplansky, *Lie Algebras and Locally Compact Groups.* Chicago: University of Chicago Press, 1971.

[5] Milne, J. S., *Algebraic Number Theory.* J.S. Milne, 2014.

[6] Neumann, B. H., *Groups Covered by Finitely Many Cosets.* Publ. Math. Debrecen 3, 1954.

[7] Ribes, Luis, *Introduction to Profinite Group.* University of Luxembourg: Winter School on Galois Theory, 2012.

[8] Ribes, L. and Zalesskii, P., *Profinite Groups.* Berlin: Springer, 2010.

[9] Soundararajan, T., *A Note on Classical Galois Theory.* Mathematische Annalen Vol. 182, 1969.

[10] Soundararajan, T., *On a Topology for a Galois System of Fields and Automorphisms.* Journal of Pure and Applied Algebra Vol. 1, No. 2, 1971.

Appendix

Proof. (van Dantzig's Theorem) Let G be a totally disconnected locally compact topological group. Firstly, we sketch out a proof that the set of all closed-open subsets of G forms a basis. Indeed, G need not be a group for this claim. Suppose that G is compact. Let $g \in G$ and H the intersection of all closed-open sets containing g. Using compactness, show that H is connected. G being totally disconnected then implies that $H = \{g\}$. Therefore, for any $h, k \in G$, there are disjoint closed-open sets H and K containing h and k respectively. Let N be a neighborhood of g. Using the compactness of G and the fact that closed-open sets separate points in G, construct a closed-open set contained in N that contains g. If G is not compact, let H be a compact neighborhood of g. Construct an open neighborhood K of g contained in H such that K is disjoint from ∂H. Use previous discussion to obtain a basis of closed-open sets contained in K.

Note that G is necessarily Hausdorff. Proceed to show that every compact open neighborhood of 1 contains a compact open subgroup using the continuity of the binary operation mapping along with compactness and the Hausdorff property. Apply the propositions given in preceding paragraph to conclude the proof. □