Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

Infinite Galois theory

Autor: Ignasi Sánchez Rodríguez

Director: Dra. Teresa Crespo
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 19 de gener de 2018

Contents

For a finite Galois extension $K \mid k$, the fundamental theorem of classical Galois theory establishes a one-to-one correspondence between the intermediate fields $E \mid k$ and the subgroups of $\mathrm{Gal}(K \mid k)$, the Galois group of the extension. With this correspondence, we can examine the finite field extension by using group theory, which is, in some sense, better understood.

A natural question may arise: does this correspondence still hold for infinite Galois extensions? It is very tempting to assume the correspondence still exists. Unfortunately, this correspondence between the intermediate fields of $K \mid k$ and the subgroups of $\mathrm{Gal}(K \mid k)$ does not necessarily hold when $K \mid k$ is an infinite Galois extension.

A naive approach to why this correspondence fails is to observe that $\mathrm{Gal}(K \mid k)$ has "too many" subgroups, so there is no subfield E of K containing k that can correspond to most of its subgroups. Therefore, it is necessary to find a way to only look at the "relevant subgroups" of the infinite Galois group. This is where topology comes to the rescue, letting us introduce a topology on an arbitrary group and study its subgroups with a different perspective.

This new study of groups with a topological perspective will lead to our main goal for this work, the discovery that the fundamental theorem of classical Galois theory holds for infinite Galois extensions $K \mid k$, whenever we associate a particular topology to the Galois group $\mathrm{Gal}(K \mid k)$.

After this theorem is proved, we are going give some examples, two of them with more details than the others. We are going to first characterize the absolute Galois group, that is, the Galois group of the extension $\overline{k} \mid k$, where $\overline{k}$ is the algebraic closure of k. This will be achieved by the means of the Artin-Shreier theorem. Then, we are going to explore the field of p-adic numbers, $\mathbb{Q}_p$. We will briefly discuss the structures of the Galois extensions of this field.

In this dissertation we assume some previous knowledge. This previous knowledge corresponds to the subjects taught at the University of Barcelona: Algebraic Structures, Algebraic Equations, Toplogy and Mathematical Analysis.

Chapter 1

Preliminaries

1.1 Topological groups

Definition 1.1. *A topological group is a set G which is both a group and a topological space and for which the map*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & xy^{-1} \end{array}$$

is continuous.

Lemma 1.2. *Let G be a topological group.*

(i) The map $(x, y) \mapsto xy$ from $G \times G$ to G is continuous and the map $x \mapsto x^{-1}$ from G to G is a homeomorphism. For each $g \in G$, the maps $x \mapsto xg$ and $x \mapsto gx$ from G to G are homeomorphisms.

(ii) If H is an open (resp. closed) subgroup of G, then every coset Hg and gH of H in G is open (resp. closed).

(iii) Every open subgroup of G is closed, and every closed subgroup of finite index is open in G. If G is compact, then every open subgroup of G has finite index.

(iv) If H is a subgroup containing a non-empty open subset U of G, then H is open in G.

(v) If H is a subgroup of G then H is a topological group with respect to the subgroup topology. If K is a normal subgroup of G, G/K is a topological group with the quotient topology and the quotient map $q : G \to G/K$ takes open sets to open sets.

(vi) G is Hausdorff if and only if $\{1\}$ is a closed subset of G and if K is a normal subgroup of G, then G/K is Hausdorff if and only if K is closed in G. If G is totally disconnected, then G is Hausdorff.

(vii) If G is compact and Hausdorff and if C, D are closed subgroups of G, then CD is closed.

(viii) *Suppose that G is compact and let $\{X_\lambda\}_{\lambda\in\Lambda}$ be a family of closed subsets with the property that, for all $\lambda_1, \lambda_2 \in \Lambda$, there exists $\mu \in \Lambda$ for which $X_\mu \subseteq X_{\lambda_1} \cap X_{\lambda_2}$. If Y is a closed subset of G, then $(\bigcap_{\lambda\in\Lambda} X_\lambda)\, Y = \bigcap_{\lambda\in\Lambda} X_\lambda Y$.*

Proof. (i) A map from a space X to $G \times G$ is continuous if and only if its product with each of the projection maps is continuous. Thus, if $\theta : \ X \longrightarrow G$ and $\varphi : \ X \longrightarrow G$ are continuous, so is the map $x \longmapsto (\theta(x), \varphi(x))$ from X to $G \times G$.

We first apply this for $\theta = 1$ and $\varphi = \mathrm{id}_G$ and compose with the continuous map $(x, y) \longmapsto xy^{-1}$:

$$\begin{array}{rccccc} x^{-1}: & G & \xrightarrow{(\theta,\varphi)} & G\times G & \xrightarrow{xy^{-1}} & G \\ & x & \longmapsto & (1,x) & \longmapsto & 1x^{-1} = x^{-1} \end{array}$$

Hence, the map $x \mapsto x^{-1}$ is continuous, and since it is its own inverse, it is a homeomorphism.

Thus, the map $(x, y) \longmapsto (x, y^{-1})$ from $G \times G$ to $G \times G$ is continuous and so is

$$\begin{array}{ccccc} G\times G & \longrightarrow & G\times G & \xrightarrow{xy^{-1}} & G \\ x & \longmapsto & (x,y^{-1}) & \longmapsto & xy \end{array}$$

Now, let $g \in G$ and take $\theta = \mathrm{id}_G$, $\varphi = g^{-1}$. Then, the composition with the continuous map from the topological group, yields the continuous map

$$\begin{array}{ccccc} G & \xrightarrow{(\theta,\varphi)} & G\times G & \xrightarrow{xy^{-1}} & G \\ x & \longmapsto & (x,g^{-1}) & \longmapsto & xg \end{array}$$

Now, taking $\theta = g$, $\varphi = 1$, we obtain the continuous map $x \longmapsto gx^{-1}$, the inverse.

We can do the same, swapping the roles of θ and φ to obtain that $x \longmapsto gx$ is a homomorphism.

(ii) Since the maps

$$\psi_g : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & xg \end{array} \qquad {}_g\psi : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gx \end{array}$$

are homeomorphisms, the result follows.

(iii) We have $G \setminus H = \bigcup\{Hg \mid g \notin H\}$. Thus, if H is open, so is $G \setminus H$ by (ii), hence H is closed. If H has a finite index, then $G \setminus H$ is a union of finitely many cosets, and thus, if H is also closed, then so is $G \setminus H$ and H is open. If H is open, then the sets Hg are open and disjoint and their union is G, thus it follows from the definition of compactness that if G is compact, then H must have finite index in G.

(iv) This follows from (ii), since for each $h \in H$, Uh is open and $H = \bigcup\{Uh \mid h \in H\}$

(*v*) The statement about H is clear, since the product is closed in H.

Now, let V be open in G. For each $k \in K$, kV is open by (ii), hence, $V_1 = KV$ is open. Thus, since $q(V) = q(V_1)$ and $q^{-1}q(V_1) = V_1$, it follows that $q(V)$ is open in G/K.

It remains to show that the map

$$\begin{array}{rccc} m: & G/K \times G/K & \longrightarrow & G/K \\ & (\xi, \zeta) & \longmapsto & \xi\zeta^{-1} \end{array}$$

is continuous. Let U be an open set in G/K and let $(K\omega_1, K\omega_2) \in m^{-1}(U)$. Since q and the map $(x, y) \mapsto xy^{-1}$ are continuous, there are open neighborhoods W_1, W_2 of ω_1, ω_2 such that $W_1 W_1^{-1} \subseteq q^{-1}(U)$ and so $q(W_1) \times q(W_2)$ is an open neighborhood of $(K\omega_1, K\omega_2)$ in $G/K \times G/K$ lying in $m^{-1}(U)$ as required.

(*vi*) We noted earlier that one-element subsets in a Hausdorff space are closed. We must show that if the set $\{1\}$ is closed in G, then G is Hausdorff. Let a, b be distinct elements of G. From (i), the set $\{ab^{-1}\}$ is closed, and so there is an open set U with $1 \in U$ and $ab^{-1} \notin U$ (in particular, the set $G \setminus \{ab^{-1}\}$ satisfies this property, since $a \neq b$). The map $(x, y) \longmapsto xy^{-1}$ is continuous and so the inverse image of U is open. It follows that there are open sets V, W containing 1 with $VW^{-1} \subseteq U$. Thus, $a^{-1}b \notin VW^{-1}$ and so $aV \cap bW = \emptyset$. Since aV, bW are open, the first assertion follows.

The other ones follow from the first, the definition of quotient topology and by the fact that if X is a totally disconnected space, then $\{x\}$ is closed in X for each $x \in X$.

(*vii*) Since C, D are closed and G is compact, both C and D are compact and so is the image of $C \times D$ under the continuous map $(x, y) \longmapsto xy$. This image is CD and since G is Hausdorff, each compact subset is closed.

(*viii*) Clearly, $\left(\bigcap X_\lambda\right) Y \subseteq \bigcap X_\lambda Y$. If $g \notin \left(\bigcap X_\lambda\right) Y$, then $gY^{-1} \cap \left(\bigcap X_\lambda\right) = \emptyset$, therefore since G is compact and gY^{-1} and X_λ are closed $\forall \lambda$, $gY^{-1} \cap X_{\lambda_1} \cap \cdots \cap X_{\{\lambda_n\}} = \emptyset$, for some finite n. However, $X_\mu \subseteq X_{\lambda_1} \cap \cdots \cap X_{\lambda_n}$ for some $\mu \in \Lambda$. Hence, $gY^{-1} \cap X_\mu = \emptyset$ and $g \notin X_\mu Y$.

□

Lemma 1.3. *Let G be a compact topological group. If C is a subset which is both closed and open and which contains 1, then C contains an open normal subgroup.*

Proof. For each $x \in C$, the set $W_x = Cx^{-1}$ is an open neighborhood of 1 such that $W_x x \subseteq C$. Since multiplication is a continuous map from $G \times G$ to G, there exists open sets L_x, R_x containing 1 such that the image of $L_x \times R_x$ is contained in W_x, i.e. such that $L_x R_x \subseteq W_x$. Let us write $S_x := L_X \cap R_x$ so that $S_x S_x \subseteq W_x$ and S_x is open. Now, C is compact and the union of open sets $C \cap S_x x$, and so it is the union of finitely many of these sets; say $C \subseteq \bigcup_{i=1}^n S_{x_i} x_i$. The set $S = \bigcap_{i=1}^n S_{x_i}$ is open and contains 1. We have

$$\subseteq \bigcup_{i=1}^{n} S S_{x_i} x_i \subseteq \bigcup_{i=1}^{n} W_{x_i} x_i \subseteq C \qquad ((1))$$

Therefore, $S \subseteq C$.

Now, let $T := S \cap S^{-1}$. Thus T is open, $T = T^{-1}$ and $1 \in T$. Write $T^1 = T$ and for $n > 1$, $T^n := TT^{n-1}$ and write $H = \bigcup_{n>0} T^n$. Thus, H is the group generated by T, and, being a union of sets of the form Ty, it is open. By induction, using (1) we have $T^n \subseteq C$, for all $n > 0$, and it follows that $H \subseteq C$. From Lemma 1.2(*iii*), H has finite index in G and so, it has only finitely many conjugates in G. The intersection of these conjugates is therefore an open normal subgroup contained in C. □

Proposition 1.4. *Let G be a compact totally disconnected topological group.*

(i) Every open set in G is a union of cosets of open normal subgroups.

(ii) A subset of G is both, closed and open if and only if it is a union of finitely many cosets of open normal subgroups.

(iii) If X is a subset of G, then

$$\overline{X} = \bigcap \{NX \mid N \text{ open normal subgroup of } G\}$$

In particular,

$$C = \bigcap \{NC \mid N \text{ open normal subgroup of } G\}$$

for each closed subset C, and the intersection of the open normal subgroups of G is the trivial subgroup.

Proof. (*i*) G is Hausdorff by Lemma 1.2(*vi*). Let U be a non-empty set in G. If $x \in U$, then Ux^{-1} is an open set containing 1, and so, by the fact that, in a disconnected space, every open set is a union of simultaneously closed and open sets, and Lemma 1.3, Ux^{-1} contains an open normal subgroup Kx. Therefore,

$$U = \bigcup_{x \in U} K_x x$$

(*ii*) If P is a set which is both closed and open, then by (i) it is a union of a family of cosets of open normal subgroups and since P is compact, it is also the union of a finite subfamily of these cosets.

Conversely, it is clear that each union of finitely many cosets of open normal subgroups is both closed and open.

(*iii*) This follows from (i) on taking complements:

If $y \notin \overline{X}$, then y has an open neighborhood disjoint from X and so there is an open normal subgroup N satisfying $Ny \cap X = \emptyset$. Hence, $y \notin NX$.

□

Lemma 1.5. *Let $\{G_\lambda \mid \lambda \in \Lambda\}$ be a family of topological groups. Let*

$$C := \prod_{\lambda \in \Lambda} G_\lambda$$

If we define multiplication in C point-wise, such that $(x_\lambda)(y_\lambda) = (x_\lambda y_\lambda)$, for all $x_\lambda, y_\lambda \in C$, then with respect with this multiplication and the product topology, C becomes a topological group.

Proof. The only thing we have to check is that the continuous function $(x_\lambda, y_\lambda) \longmapsto x_\lambda y_\lambda$ from $G_\lambda \times G_\lambda$ to G_λ extends to a continuous function in C. But this is trivial, since we have the following

$$\begin{array}{ccccc} C \times C & \xrightarrow{p_\lambda \times p_\lambda} & G_\lambda \times G_\lambda & \longrightarrow & G_\lambda \\ ((x_\lambda),(y_\lambda)) & \longmapsto & (x_\lambda, y_\lambda) & \longmapsto & x_\lambda y_\lambda^{-1} \end{array}$$

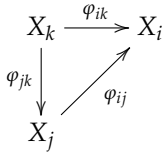
where p_λ is the projection from C to G_λ and hence, the composition is continuous for each $\lambda \in \Lambda$, therefore, so is the map $((x_\lambda),(y_\lambda)) \longmapsto (x_\lambda y_\lambda^{-1})$. □

1.2 Inverse Limits

Definition 1.6. *We say that a partially ordered set (poset) $\langle I, \leq \rangle$ is a directed set if, for every $i_1, i_2 \in I$, there exists $j \in I$ for which $i_1 \leq j$ and $i_2 \leq j$.*

Definition 1.7. *Let $\mathcal{C}$ be a category. An inverse system (X_i, φ_{ij}) of $\mathcal{C}$ indexed by a directed set I consists of:*

- *A subset of $Ob(\mathcal{C})$ indexed by I, $\{X_i \mid i \in I\}$.*
- *A family of $Ar(\mathcal{C})$, $\{\ \varphi_{ij} : \ X_j \longrightarrow X_i \ \mid i, j \in I,\ i \leq j\}$, such that $\varphi_{ii} = \mathrm{id}_{X_i}$ for all $i \in I$ and the following diagram is commutative whenever $i \leq j \leq k$*



Remark 1.8. If each X_i is a topological space (resp. topological group) and each φ_{ij} is a continuous function (resp. continuous homomorphism), (X_i, φ_{ij}) is called an inverse system of topological spaces (resp. topological groups).

Example 1.9. (1) Let $I = \mathbb{N}$, $p \in \mathbb{Z}$ prime, $G_i = {}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}}$ and for $j \geq i$, let

$$\begin{array}{rccc} \varphi_{ij} : & G_j & \longrightarrow & G_i \\ & n + p^j\mathbb{Z} & \longmapsto & n + p^i\mathbb{Z} \end{array}$$

Then, (G_i, φ_{ij}) is an inverse system of finite groups.

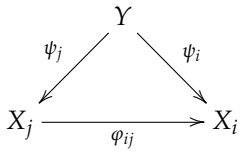
(2) As a more general example, let G be a group and let I be the family of normal subgroups with the property that for each $U_1, U_2 \in I$, there exists $V \in I$ such that $V \subseteq U_1 \cap U_2$. We may regard I as a directed set with respect to the order $\leq'$, defined as: $U \leq' V$ if and only if V is a subgroup of U.

Now, for $U \leq' V$, let

$$q_{UV}: \begin{array}{ccc} G/V & \longrightarrow & G/U \\ Vg & \longmapsto & Ug \end{array}$$

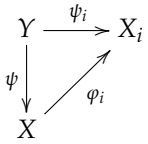
Then (G_U, q_{UV}) is an inverse system of groups.

Definition 1.10. *Let $(X_i, \varphi_{i,j})$ be an inverse system of a category $\mathcal{C}$ indexed by I and let Y be an element of $Ob(\mathcal{C})$. We shall call a family $\{\ \psi_i : \ Y \longrightarrow X_i \ \mid i \in I\}$ of arrows of $\mathcal{C}$ compatible if the following diagram is commutative*



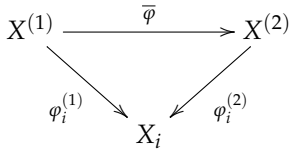
Definition 1.11. *An inverse limit (X, φ_i) of an inverse system (X_i, φ_{ij}) of a category $\mathcal{C}$ is an object X of $\mathcal{C}$ together with a compatible family $\{\ \varphi_i : \ X \longrightarrow X_i\ \}$ of arrows of $\mathcal{C}$ that satisfy the universal property:*

Whenever $\{\ \psi_i : \ Y \longrightarrow X_i\ \}$ is a compatible family of arrows of $\mathcal{C}$ from an object of $\mathcal{C}$, Y, there exists a unique arrow of $\mathcal{C}$ $\psi : \ Y \longrightarrow X$ that makes the following diagram commutative



Proposition 1.12. *Let (X_i, φ_{ij}) be an inverse system indexed by I.*

(i) If $(X^{(1)}, \varphi_i^{(1)})$ and $(X^{(2)}, \varphi_i^{(2)})$ are inverse limits of the inverse system, then there is an isomorphism $\overline{\varphi} : \ X^{(1)} \longrightarrow X^{(2)}$ such that the diagram is commutative



(ii) We write $C := \prod_{i \in I} X_i$ and, for every $i \in I$, write π_i the projection from C to X_i. Then, define

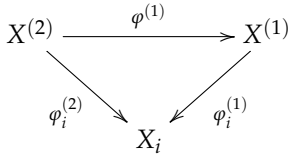
$$X = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c),\ i \leq j\}$$

and $\varphi_i = \pi_i|_X$ for each $i \in I$. Then (X, φ_i) is an inverse limit of (X_i, ϕ_{ij}).

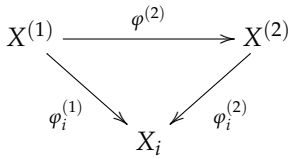
(iii) If (X_i, φ_{ij}) is an inverse system of topological groups and continuous homomorphisms, then X is a topological group and the maps φ_i are continuous homomorphisms.

Proof. (*i*) This follows from the uniqueness of the universal property.

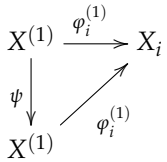
The universal property of $(X^{(1)}, \varphi_i^{(1)})$ applied to the family $\{\varphi_i^{(2)}\}$ of compatible maps yields a map $\varphi^{(1)} : X^{(2)} \longrightarrow X^{(1)}$ such that the diagram is commutative for each $i \in I$



Similarly, the universal property of $(X^{(2)}, \varphi_i^{(2)})$ applied to the family $\{\varphi_i^{(1)}\}$ of compatible maps yields a map $\varphi^{(2)} : X^{(1)} \longrightarrow X^{(2)}$ such that the diagram is commutative for each $i \in I$



Now, by the universal property of $(X^{(1)}, \varphi_i^{(1)})$, the map $\psi : X^{(1)} \longrightarrow X^{(1)}$ making the diagram commutative for each $i \in I$



is unique. But, the composition $\varphi^{(1)}\varphi^{(2)}$ and $\mathrm{id}_{X^{(1)}}$ both satisfy it. Hence, $\varphi^{(1)}\varphi^{(2)} = \mathrm{id}_{X^{(1)}}$.

In the same manner, we obtain $\varphi^{(2)}\varphi^{(1)} = \mathrm{id}_{X^{(2)}}$.

It follows that $\varphi^{(1)}$ and $\varphi^{(2)}$ are both arrows of $\mathcal{C}$ and inverse one form another. Particularly, $\overline{\varphi} = \varphi^{(2)}$.

(*ii*) We will prove this for topological spaces. The general proof using Category Theory needs a bit more theory so that we can define direct products in a category. We regard C as equipped with the product topology and X with the subspace topology. Thus, the maps φ_i are certainly continuous and the definition of X ensures that $\varphi_{ij}\varphi_j = \varphi_i$ whenever $j \geq i$.

Suppose that $\{\ \psi_i : Y \longrightarrow X_i\ \}$ is a compatible family of continuous maps. We must show that there is a unique continuous map $\psi : Y \longrightarrow X$ such that $\varphi_i\psi = \psi_i$ for each i. Let $\overline{\psi}$ be the map from Y to C taking $y \in Y$ to $\psi_i(y)$. Thus $\pi_i\overline{\psi} = \psi_i$, for each i and ψ is continuous because ψ_i and π_i are continuous for each i.

Now, if $j \geq i$, then

$$\pi_i \overline{\psi} = \psi_i = \varphi_{ij}\psi_j = \varphi_{ij}\pi_j\overline{\psi}$$

and it follows that $\overline{\psi}$ maps Y into X.

Define $\psi : \quad Y \longrightarrow X$ by $\psi(y) := \overline{\psi}(y)$, for any $y \in Y$. Thus, ψ is continuous and $\varphi_i\psi = \psi_i$ for each i.

Finally, if $\psi' : \quad Y \longrightarrow X$ is a map satisfying $\varphi_i\psi' = \psi_i$ for each i, then the entry in X_i of $\psi'(y)$ is $\psi_i(y)$ for each i, hence $\psi'(y) = \psi(y)$ for every $y \in Y$.

(*iii*) This comes trivially combining (ii) and (i) and noting that in (ii), if (X_i, φ_{ij}) is an inverse system of groups and continuous homomorphisms, and the maps $\psi_i : \quad Y \longrightarrow X_i$ are group homomorphisms, then so is ψ.

□

Notation. *We have shown that the inverse limit is unique mod isomorphism. In some cases, when we try to find the limit, it will be easier to use the special limit found in* (ii)*. We will refer to it as* $\varprojlim$.

Proposition 1.13. *Let* (X_i, φ_{ij}) *be an inverse system of topological spaces, indexed by* I*, and write* $X = \varprojlim X_i$.

(i) If each X_i *is Hausdorff, so is* X.

(ii) If each X_i *is totally disconnected, so is* X.

(iii) If each X_i *is Hausdorff, then* $\varprojlim X_i$ *is closed in the cartesian product* $C = \prod_{i\in I} X_i$.

(iv) If each X_i *is compact and Hausdorff, so is* X.

(v) If each X_i *is non-empty compact Hausdorff, then* X *is non-empty.*

Proof. If we consider $X' = \varprojlim X_i$, then there is an isomorphism between X and X'. Hence, proving that X' has any topological property it translates to X having it.

(*i*) Since $X' \subseteq \prod_{i\in I} X_i$, the Cartesian product maintains the Hausdorff property and any subset of a Hausdorff space is Hausdorff, then X' is Hausdorff.

(*ii*) Since $X' \subseteq \prod_{i\in I} X_i$, the Cartesian product maintains the totally disconnected property and any subset of a totally disconnected space is totally disconnected, then X' is totally disconnected.

(*iii*) If $f, g : \quad X \longrightarrow Y$ are continuous maps and Y is Hausdorff, then the set $\{x \in X \mid f(x) = g(x)\}$ is closed in X.

Since

$$\varprojlim X_i = \bigcap_{j>i} \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c)\}$$

where the maps π_i are the projection maps, it follows that if each X_i is Hausdorff, then $\varprojlim X_i$ is the intersection of closed sets and hence is closed in the Cartesian product.

(*iv*) Follows from (iii), (i), the fact that the Cartesian product of compact spaces is compact and that each closed subset of a compact space is compact.

(*v*) For each $j > i$, define $D_{ij} := \{x \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c)\}$. Each D_{ij} is closed and C is compact, and so, if $\varprojlim X_i = \emptyset$, then $\bigcap_{r=1}^{n} D_{i_r j_r} = \emptyset$ for some integer n and elements $i_r, j_r \in I$. Since I is directed, we can find $k \in I$ such that $k \geq j_r$, for every r. We choose $x_k \in X_k$ and we define $x_l = \varphi_{lk}(x_k)$ for $l \leq k$ and define x_l arbitrarily for all other elements of I. Clearly, the element (x_i) of the Cartesian product lies in $\bigcap_{r=1}^{n} D_{i_r j_r}$ and this contradiction finishes the proof.

□

Proposition 1.14. *Let (X, φ_i) be the inverse limit of the inverse system of topological spaces (X_i, φ_{ij}) of non-empty compact Hausdorff spaces indexed by I. The following assertions hold*

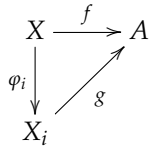
(i) $\varphi_i(X) = \bigcap_{j \geq i} \varphi_{ij}(X_j)$, *for every* $i \in I$.

(ii) *The sets* $\varphi_i^{-1}(U)$ *with* $i \in I$ *and* U *open in* X_i *form a base 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) *If* θ *is a map from a space* Y *to* X, *then* θ *is continuous if and only is* $\varphi_i\theta$ *is continuous.*

(v) *If* $f : X \longrightarrow A$ *is a continuous map to a discrete space* A, *then* f *factors through* X_i *for some* $i \in I$. *That is there exists* $g : X_i \longrightarrow A$ *so that the following diagram commutes*



Proof. We are going to use the notation from the last proposition. Therefore, let $X = \varprojlim X_i$, $C = \prod_{i \in I} X_i$ and π_i the projection maps from C to X_i for each i such that $\varphi_i = \pi_i|_X$.

(*i*) We have $\varphi_i(X) = \varphi_{ij}\varphi_j(X) \subseteq \varphi_{ij}(X)$ for all $j \geq i$ and therefore $\varphi_i(X) \subseteq \bigcap_{j \geq i} \varphi_{ij}(X_j)$. Now, fix i and $a \in \bigcap_{j \geq i}(X_j)$ for $j \geq i$, set

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

Thus Y_j, being the inverse image of a closed set is closed in X_j and hence compact.

If $i \leq j \leq k$ and $y_k \in Y_k$, then $\varphi_{ij}\varphi_{jk}(y_k) = \varphi_{ik}(y_k) = a$, hence $\varphi_{ik}(y_k) \in Y_k$.

Therefore, $\{Y_j \mid j \geq i\}$ is, with respect to the restrictions of the maps φ_{ij}, an inverse system of non-empty compact Hausdorff spaces and so, there is an element $(b_j) \in \varprojlim_{j \geq i} X_i$. Thus, $\varphi_{jk}(b_k) = b_j$ if $i \leq j \leq k$ and $b_i = a$.

(*ii*) Every open set in X is a union of sets of the form

$$P = X \cap \pi_{i_1}^{-1}(U_1) \cap \cdots \cap \pi_{i_n}^{-1}(U_n)$$

with n an integer, $i_1, \ldots, i_n \in I$ and U_r open in X_{i_r} for each r.

The result will follow if we can prove that for all $a \in P$, there is an open set $\varphi_k^{-1}(U)$ with U an open set in X_k, and $a \in \varphi_k^{-1}(U) \subseteq P$.

Let $a = (a_i)$. Choose $k \in I$ such that it contains a_k, since $\varphi_{ik}(a_k) = a_i$ for $i \leq k$. Write

$$U = \bigcap_{r=1}^{n} \varphi_{i_r k}^{-1}(U_r)$$

This is an open neighborhood of a_k in X_k and so $\varphi_k^{-1}(U)$ is an open neighborhood of a in X. However, if $b = (b_i) \in \varphi_k^{-1}(U)$, then $b_k \in U$ so that $b_{i_r} = \varphi_{i_r k}(b_k) \in U_r$ for $r = 1, \ldots, n$. It follows that $\varphi_k^{-1}(U) \subseteq P$.

(*iii*) For each $i \in I$ and each non-empty open set U in X_i, we clearly have $\varphi(Y) \cap U \neq \emptyset$ and hence, $Y \cap \varphi_i^{-1}(U) \neq \emptyset$. It follows from (ii) that Y is dense in X.

(*iv*) Clearly if θ is continuous then so is each map $\varphi_i\theta$.

Conversely, if $\varphi_i\theta$ is continuous, then for each $i \in I$ and each open set U in X_i, the set $\theta^{-1}\varphi_i^{-1}(U) = (\varphi_i\theta)(U)$ is open and it follows from (ii) that θ is continuous.

(*v*) The image A_0 of f is compact and discrete, hence, finite. For each $a \in A_0$, the set $Y_a = f^{-1}(a)$ is compact and open, and so, it is a finite union of open sets $\varphi_j^{-1}(U)$ with $j \in I$ and U open in X_j. Thus, there are finitely many sets $\varphi_{j_1}^{-1}(U_1), \ldots, \varphi_{j_n}^{-1}(U_n)$ such that the set Y_a us the union of some of these sets.

Choose k such that $j_r \leq k$ for $r = 1, \ldots, n$. We have $\varphi_{j_r}^{-1}(U_r) = \varphi_k^{-1}(\varphi_{j_r k}^{-1}(U_r))$ for each r, and so, for each $a \in A_0$ we can write

$$Y_a = \varphi_k^{-1}(V_a)$$

where V_a is an open subset of X_k. Write

$$D = X_k \setminus \bigcup_{a \in A_0} V_a$$

Clearly, $D \cap \varphi_k(X) = \emptyset$ and so, by (i), we have $D \cap \left(\bigcap_{l \geq k} \varphi_{kl}(X_l)\right)$. Therefore, there are finitely many indices $l_1, \ldots, l_s$ such that

$$D \cap \varphi_{kl_1}(X_{l_1}) \cap \cdots \cap \varphi_{kl_s}(X_{l_s}) = \emptyset$$

since D an each set $\varphi_{kl}(X_l)$ is closed and X_k compact.

We choose $i \geq l_1, \ldots, l_s$. For $k \leq l \leq i$, we have

$$\varphi_{ki}(X_i) = \varphi_{kl}(\varphi_{li}(X_i)) \subseteq \varphi_{kl}(X_k)$$

and conclude

$$D \cap \varphi_{ki}(X_i) = \emptyset \quad \text{and} \quad \varphi_{ki}(X_i) \subseteq \bigcup_{a \in A_0} V_a$$

Write $W_a = \varphi_{ki}^{-1}(V_a)$ for each a. Thus, each W_a is open in X_i and clearly $W_{a_1} \cap W_{a_2} = \emptyset$ for $a_1 \neq a_2$.

Let $x \in \varphi_{ki}^{-1}(W_a)$. Therefore,

$$X_i = \bigcup_{a \in A_0} W_a$$

and each set W_a is also closed. It follows that the map $\begin{array}{rccc} g: & X_i & \longrightarrow & A \\ & W_a & \longmapsto & a \end{array}$ for each $a \in A_0$ is continuous and satisfies $f = g\varphi_i$.

□

Theorem 1.15. *Let X be a compact Hausdorff totally disconnected space, Then X is the inverse limit of its discrete quotient spaces.*

Proof. Let I be the set of all partitions of X into finitely many closed and open subsets. For each $i \in I$, let X_i be the corresponding quotient space (whose elements are closed and open sets of the partition i) and let q_i be the quotient map form X to X_i.

Since this might not be clear, let us exemplify it: Let X be a space and $X_i, X_j \in I$ two different partitions of X. As an example, let us take

$$X_i = \{X_i^1, X_i^2, X_i^3, X_i^4\}, \qquad X_i^1, X_i^2, X_i^3, X_i^4 \subseteq X, \qquad X_i^1 \cup X_i^2 \cup X_i^3 \cup X_i^4 = X$$

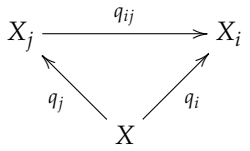
and

$$X_j = \{X_j^1, X_j^2, X_j^3\}, \qquad X_j^1, X_j^2, X_j^3 \subseteq X, \qquad X_j^1 \cup X_j^2 \cup X_j^3 = X$$

Now, the quotient maps are

$$\begin{array}{rccc} q_i: & X & \longrightarrow & X_i \\ & x \in X_i^k & \longmapsto & X_i^k \end{array} \qquad \begin{array}{rccc} q_j: & X & \longrightarrow & X_j \\ & x \in X_j^k & \longmapsto & X_j^k \end{array}$$

Following with the proof, the sets X_i are precisely the quotient spaces of X which are discrete in the quotient topology. We write $i \leq j$ if and only if, there is a map $q_{ij}: X_j \longrightarrow X_i$ satisfying the commutativity of the diagram



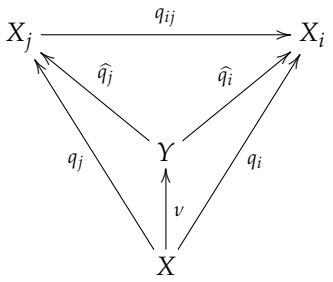
The map q_{ij} is uniquely determined since q_j is exhaustive.

Now, the set $\langle I, \leq \rangle$ is a partially ordered set. Then, if $i = \{U_r \mid 1 \leq r \leq m\}$ and $j = \{V_s \mid 1 \leq s \leq n\}$ are elements of I, then the set $k = \{U_r \cap V_s \mid 1 \leq r \leq m, 1 \leq s \leq n\}$ is also an element of I such that $i, j \leq k$. Hence I is a directed set.

Since each map q_{ij} is uniquely determined, it follows at once that (X_i, q_{ij}) is an inverse system and that (q_i) is a compatible family of maps. Particularly, (X, q_i) is a candidate to be the inverse limit of the inverse system.

Let $Y = \varprojlim X_i$ and let $\widehat{q_i} : \quad Y \longrightarrow X_i$ be the canonical map for each i. The universal property of the inverse limit yields a continuous map $\nu : \quad X \longrightarrow Y$ such that $\widehat{q_i}\nu = q_i$ for each i.

Hence, we have the following diagram



We will end the proof showing that ν is an isomorphism. Let $x_1, x_2 \in X$ such that $\nu(x_1) = \nu(x_2)$. Now, $\widehat{q_i}(\nu(x_1)) = \widehat{q_i}(\nu(x_2))$ for each i implies $q_i(x_1) = q_i(x_2)$ for each i. This implies that no open or closed sets contains just one of x_1, x_2, thus $x_1 = x_2$ since X is totally disconnected. This implies that ν is injective.

Now, since $\widehat{q_i}(\nu(X)) = q_i(X) = X_i$, it follows from Proposition 1.14(iii) that $\nu(X)$ is dense in Y and since ν is continuous, X is compact and Y is Hausdorff, $\nu(X)$ is closed, hence $\nu(X) = \overline{\nu(X)} = Y$. This implies that ν is surjective. □

1.2.1 Examples of projective limits

The p-adic integers $\mathbb{Z}_p$

Let p be a prime number. Let us define the inverse system of rings $\left(\mathbb{Z}/p^n\mathbb{Z}, \varphi_{nm}\right)$, where $m \geq n$ and

$$\begin{array}{rccc} \varphi_{nm} : & \mathbb{Z}/p^m\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} \\ & x + p^m\mathbb{Z} & \longmapsto & x + p^n\mathbb{Z} \end{array}$$

Now, we would like to compute $\widehat{\mathbb{Z}_p} := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

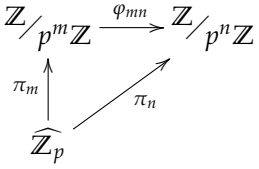
Being the $\varprojlim$, $\widehat{\mathbb{Z}_p}$ satisfies two conditions:

The first one,

$$\widehat{\mathbb{Z}_p} \subseteq \prod_{n \in \mathbb{N}_{>0}} \mathbb{Z}/p^n\mathbb{Z}$$

Hence, if $z \in \widehat{\mathbb{Z}_p}$, then $z = (a_1, a_2, \ldots, a_n, \ldots)$, with $a_i \in \mathbb{Z}/p^i\mathbb{Z}$, i.e. $0 \leq a_i < p^i$. The second one is that, for every two positive integers m, n, with $m \geq n$ the following diagram

is commutative



where π_i are the projection maps. Now, this implies that, for any $z \in \widehat{\mathbb{Z}_p}$, $\varphi_{n(n+1)}(\pi_{n+1}(z)) = \pi_n(z)$. That is, if $z = (a_1, a_2, \dots)$, then $\varphi_{n(n+1)}(a_{n+1}) = a_n$. Now, since $a_i \in \mathbb{Z}/p^i\mathbb{Z}$, we can write a_i as $a_i + p^i\mathbb{Z}$. Hence, $\varphi_{n(n+1)}(a_{n+1} + p^{n+1}\mathbb{Z}) = a_n + p^n\mathbb{Z}$. By the definition of $\varphi_{n(n+1)}$, we have $a_{n+1} + p^n\mathbb{Z} = a_n + p^n\mathbb{Z}$. This yields the result

$$a_{n+1} \equiv a_n \pmod{p^n}, \qquad \forall\, n \in \mathbb{N}_{n\geq 0}$$

Therefore, each element $z \in \widehat{\mathbb{Z}_p}$ can be written as $(a \pmod{p}, a \pmod{p^2}, \dots, a \pmod{p^n}, \dots)$, for some $a \in \mathbb{Z}$.

Definition 1.16. *We define a p-adic integer as the formal infinite sum*

$$a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \dots$$

with $0 \leq a_i < p$, for each $i \in \mathbb{N}$. We denote the set of all p-adic integers as $\mathbb{Z}_p$.

Proposition. *The residue classes of $a \pmod{p^n}$ can be uniquely represented in the form*

$$a \equiv a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \pmod{p^n}$$

where $0 \leq a_i < p$, with $i = 0, \dots, n-1$.

Proof. Let us do induction on n. For $n = 1$, the result is clear since $a \equiv a_0 \pmod{p}$ uniquely.

Assume the statement to be proved for $n-1$. Then, we have

$$a = a_0 + a_1 p + a_2 p^2 + \dots a_{n-2} p^{n-2} + g p^{n-1}$$

for some $g \in \mathbb{Z}$. If we define a_{n-1} as $g \equiv a_{n-1} \pmod{p}$, it is uniquely determined and this proves the proposition. □

Now, we see a lot of similarities between $\widehat{\mathbb{Z}_p}$ and $\mathbb{Z}_p$. In fact, the following results gives us the relation we're looking for

Theorem. *There is bijection between $\widehat{\mathbb{Z}_p}$ and $\mathbb{Z}_p$. In fact, this bijection preserves the topological group structure of $\widehat{\mathbb{Z}_p}$, hence $\mathbb{Z}_p$ is also a topological group.*

Proof. For each element of $\mathbb{Z}_p$, $\sum_{i=0}^{\infty} a_i p^i$, we can define the partial sums $s_n = \sum_{i=0}^{n-1} a_i p^i$ and moreover, their residual classes $\overline{s_n} \equiv s_n \pmod{p^n}$. Now, every one of these $\overline{s_n}$ is an element of $\mathbb{Z}/p^n\mathbb{Z}$, hence, we can write every element of $\mathbb{Z}_p$ in $\widehat{\mathbb{Z}_p}$ using this. That is, the map from $\mathbb{Z}_p$ to $\widehat{\mathbb{Z}_p}$

$$\sum_{i=0}^{\infty} a_i p^i \longmapsto (\overline{s_0}, \overline{s_1}, \dots)$$

We also note that $\varphi_{n(n+1)}(\overline{s_{n+1}}) = \overline{s_n}$.

For the other map, we just have to use the fact that every element of $\widehat{\mathbb{Z}_p}$ can be written as $(a \pmod p), a \pmod{p^2}, \dots)$ and using the proposition, we can send this element to $a_0 + a_1 p + a_2 p^2 + \dots$, where $a \equiv a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \pmod{p^n}$, for every $n \in \mathbb{N}$. This is well defined by recursion, hence, we have the map from $\widehat{\mathbb{Z}_p}$ to $\mathbb{Z}_p$

$$(a \pmod p), a \pmod{p^2}, \dots) \longmapsto s_0 + s_1 p + \dots$$

These two maps are inverse one from another, therefore, there is a bijection between $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}_p}$.

It can also be easily shown that the topological group structure is passed onto $\mathbb{Z}_p$.

□

Remark. *The ring $\mathbb{Z}_p$ may also be obtained by $\mathbb{Z}$ using the p-adic norm. We will expand on this topic on Chapter* 4.

The Prüfer ring $\widehat{\mathbb{Z}}$

Let us consider the poset $\langle \mathbb{N}, | \rangle$, where $|$ is the divisibility relation, i.e., if $n, m \in N$, then $n \mid m$ if and only if $m = kn$ for some $k \in \mathbb{N}$. Then, if $m \geq n$, we define the morphism

$$\varphi_{nm} : \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ a + m\mathbb{Z} & \longmapsto & a + n\mathbb{Z} \end{array}$$

This is well defined since $n \mid m$. Hence, $\left(\mathbb{Z}/n\mathbb{Z}, \varphi_{nm}\right)$ is a projective system of topological groups.

The projective limit of this system is the Prüfer ring or how its called nowadays, the zed-hat ring, denoted as $\widehat{\mathbb{Z}}$.

This topological group has some properties:

- $\mathbb{Z}$ is a dense open subgroup of $\widehat{\mathbb{Z}}$.
- $n\widehat{\mathbb{Z}}$ are the open subgroups of $\widehat{\mathbb{Z}}$, for each $n \in \mathbb{N}$.
- Using the Chinese Remainder Theorem, if $n = \prod_p p^{s_i}$, then

  $$\mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}/p^{s_i}\mathbb{Z}$$

  Taking projective limits on both sides, we obtain

  $$\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$$

Some results are derived from these properties:

(1) We know that $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$ for any $n \in \mathbb{N}$ mapping the Frobenius automorphism $\varphi_n(x) = x^q$ of $\mathbb{F}_{q^n}$ to $1 \in \mathbb{Z}/n\mathbb{Z}$.

Passing to the projective limit, we have the result

$$\mathrm{Gal}(\overline{\mathbb{F}_q} \mid \mathbb{F}_q) \cong \widehat{\mathbb{Z}}$$

Remark. $\varinjlim \mathbb{F}_{q^n} = \overline{\mathbb{F}_q}$ *the algebraic closure of* $\mathbb{F}_q$. $\varinjlim$ *is called the direct limit. We define a directed system in a similar manner as an inverse system, but instead of having arrows* $\varphi_{ij} : X_j \longrightarrow X_i$ *whenever* $i \leq j$*, we have* $\varphi_{ij} : X_i \longrightarrow X_j$ *whenever* $i \leq j$*. The definition of the directed limit follows: Let* $\left(X_i, \varphi_{ij}\right)$ *be a direct system of objects and morphisms in* $\mathcal{C}$*. A direct limit is a pair* (X, φ_i) *where* X*, is an object in* $\mathcal{C}$ *and* $\varphi_i : X_i \longrightarrow X$ *are morphisms such that* $\varphi_i = \varphi_j \circ \varphi_{ij}$ *(i.e. they are compatible) and satisfy the universal property.*

Remark. *This isomorphism sends the Frobenius automorphism* φ *of* $\overline{\mathbb{F}_q}$ *to* $1 \in \widehat{\mathbb{Z}}$ *and the subgroup* $\langle \varphi \rangle$ *to* $\mathbb{Z}$*. This last assertion is important, since it says that we can find* $\psi \in \mathrm{Gal}(\overline{\mathbb{F}_q} \mid \mathbb{F}_q)$ *such that* $\psi \notin \langle \varphi \rangle$*, which is a contradiction to the classical Galois Fundamental Theorem, as we are going to see in Chapter 2.*

(2) Let $\widetilde{\mathbb{Q}} \mid \mathbb{Q}$ be the extension obtained by adjoining all roots of unity. We know, from classical Galois Theory that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q}) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

where ζ_n is an nth root of unity. Taking projective limits on both sides, and assuming $\varprojlim \left(\mathbb{Z}/n\mathbb{Z}\right)^* \cong \widehat{\mathbb{Z}}^*$, we obtain

$$\mathrm{Gal}(\widetilde{\mathbb{Q}} \mid \mathbb{Q}) \cong \widehat{\mathbb{Z}}^*$$

1.3 Profinite groups

Definition 1.17. *We call a family* I *of normal open subgroups of an arbitrary group* G *a filter base if, for every* $k_1, k_2 \in I$*, there exists* $k_3 \in I$ *contained in* $k_1 \cap k_2$*.*

Proposition 1.18. *Let* (G, φ_i) *be the inverse limit of an inverse system* (G_i, φ_{ij}) *of compact Hausdorff topological groups indexed by* I*. Let* L *be an open normal subgroup of* G*. Then* $\ker \varphi_i$ *is a closed subgroup of* L *for some* i*. Consequently,* G/L *is isomorphic, as a topological group, to a quotient group of a subgroup of some* G_i*, and if, in addition, each map* φ_i *is surjective, then* G/L *is isomorphic to a quotient group of some* G_i*.*

Proof. Since L is open and contains 1, we have $\varphi_i^{-1}(U) \subseteq L$ for some i and some open set U of G_i containing 1 (everything comes from Proposition 1.14(ii)). Therefore, $\ker \varphi_i$ is a closed subgroup of L for some I. Thus we have

$$G/L \cong \left(G/\ker \varphi_i\right)\Big/\left(L/\ker \varphi_i\right)$$

Since $G/\ker \varphi \cong \mathrm{Im}\, \varphi_i$ it follows that G/L is isomorphic to a quotient of $\mathrm{Im}\, \varphi_i$. The other assertion follows. □

Proposition 1.19. *Let G be a topological group and I a filter base of closed normal subgroups. For $K, L \in I$, define $K \leq' L$ if and only if $L \subseteq K$. Now, I is directed with respect to $\leq'$ and the surjective homomorphisms $q_{KL} : {}^{G}\!/_{L} \longrightarrow {}^{G}\!/_{K}$ defined for $K \leq' L$, make the groups ${}^{G}\!/_{K}$ into an inverse system.*

Write $(\widehat{G}, \varphi_k) = \varprojlim \left({}^{G}\!/_{K}, q_{KL}\right)$.

There is a continuous homomorphism $\theta : G \longrightarrow \widehat{G}$ with kernel $\bigcap_{K\in I} K$ with image a dense subgroup of $\widehat{G}$ and such that $\varphi_K\theta$ is the quotient map from G to ${}^{G}\!/_{K}$.

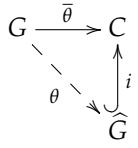
If G is compact, then θ is surjective, $\bigcap_{K\in I} K = 1$ and θ is an isomorphism of topological groups.

Proof. We proved in Theorem 1.15 that $\left({}^{G}\!/_{K}, q_{KL}\right)$ is an inverse system. We shall take $\widehat{G} = \varprojlim {}^{G}\!/_{K}$. Now, the map

$$\begin{array}{rccc} \overline{\theta}: & G & \longrightarrow & C := \prod_{K\in I} {}^{G}\!/_{K} \\ & g & \longmapsto & (gK) \end{array}$$

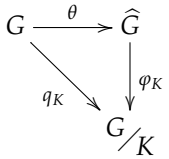
has $\mathrm{Im}(\overline{\theta}) \subseteq \widehat{G}$.

This gives an induced map from G to $\widehat{G}$



Now, since $q_k = \pi_k\overline{\theta}$ and q_k and π_k are continuous homomorphisms, then $\overline{\theta}$ is a continuous homomorphism, hence θ is a continuous homomorphism.

Let $g \in G$, $g \in \mathrm{Ker}\,\theta$ if and only if $Kg = K$, for every $K \in I$. Hence, $\mathrm{Ker}\,\theta = \bigcap_{K\in I} K$. For each $K \in I$, $\varphi_K(\theta(G)) = {}^{G}\!/_{K}$. Hence, the diagram commutes



Now, by Proposition 1.14(iii), $\mathrm{Im}\,\theta$ is dense in $\widehat{G}$.

By Lemma 1.2(vi) each group ${}^{G}\!/_{K}$ with $K \in I$ is Hausdorff.

Finally, suppose G compact. Then $\theta(G)$ is compact, hence $\theta(G)$ is closed in C. Since $\theta(G)$ is also dense in $\widehat{G}$, it follows $\theta(G) = \widehat{G}$.

If, in addition $\bigcap_{K\in I} K = 1$, then θ is a continuous bijection and so, a homeomorphism, since G is compact and $\widehat{G}$ Hausdorff. □

Definition 1.20. *A class of finite groups is a class in the usual sense which, in addition, is closed with respect to taking isomorphic images.*

That is, if $\mathcal{C}$ is a class, $F_1 \in \mathcal{C}$, and $F_2 \cong F_1$, then $F_2 \in \mathcal{C}$.

Definition 1.21. *Let $\mathcal{C}$ be a class of finite groups.*
We call a group F a $\mathcal{C}-$group if $F \in \mathcal{F}$.
We call a group G a pro$-\mathcal{C}$ group if it is an inverse limit of $\mathcal{C}-$groups.

Definition 1.22. *We say that $\mathcal{C}$ is closed for subgroups (resp. quotients) if every subgroup (resp. quotient) of a $\mathcal{C}-$group is again a $\mathcal{C}-$group.*

Definition 1.23. *We say that $\mathcal{C}$ is closed for direct products if $F_1 \times F_2 \in \mathcal{C}$ whenever $F_1, F_2 \in \mathcal{C}$*

We shall now characterize the pro$-\mathcal{C}$ groups.

Theorem 1.24. *Let $\mathcal{C}$ be a class of finite groups which is closed for subgroups and directed products, and let G be a topological group. The following are equivalent:*

(i) *G is a pro$-\mathcal{C}$ group.*

(ii) *G is isomorphic (as a topological group) to a closed subgroup of a cartesian product of $\mathcal{C}-$groups.*

(iii) *G is compact and $\bigcap\{N \mid N$ is an open normal subgroup of G and $G/N \in \mathcal{C}\} = 1$.*

(iv) *G is compact and totally disconnected, and for every open normal subgroup L of G, there is a normal subgroup N of G with N closed in L and $G/N \in \mathcal{C}$.*

In addition, if $\mathcal{C}$ is closed for quotients, then (iv) can be replaced by

(iv') *G is compact and totally disconnected and $G/L \in \mathcal{C}$ for every open normal subgroup L of G.*

Proof.

$(i) \Rightarrow (ii)$ This follows from Proposition 1.13(iii).

$(ii) \Rightarrow (iii)$ Let G be isomorphic to $\widehat{G}$, a closed subgroup of $C = \prod G_i$, where each $G_i \in \mathcal{C}$. For each i, write K_i for the kernel of the projection map from C to G_i. Since each G_i is compact, C is compact, hence, $\widehat{G}$ is compact.

For each i, write $N_i = K_i \cap \widehat{G}$. Since K_i is an open normal subgroup of C, so is N_i; and since $\bigcap K_i = 1$, we have $\bigcap N_i = 1$. Moreover,

$$\widehat{G}/N_i \cong GK_i/K_i \subseteq C/K_i \cong G_i$$

where GK_i/K_i is a closed subgroup of C/K_i. Hence, $\widehat{G}/N_i \in \mathcal{C}$ for each i.

$(iii) \Rightarrow (i)$ Write $I = \{N \mid N$ is an open normal subgroup of G and $G/N \in \mathcal{C}\}$. Let $N_1, N_2 \in I$ and consider the map from G to the $\mathcal{C}$-group $G/N_1 \times G/N_2$ defined by $g \longmapsto (N_1 g, N_2 g)$. This is a continuous homomorphism and its kernel is $N_1 \cap N_2$. It follows that $N_1 \cap N_2 \in I$. Therefore, Proposition 1.19 may be applied and we have $G \cong \varprojlim_{N \in I} G/N$.

$(i) \Rightarrow (iv)$ By Proposition 1.13, G is compact and totally disconnected and the remaining follows from Proposition 1.18.

$(iv) \Rightarrow (iii)$ This follows from Proposition 1.4.

Finally, suppose that $\mathcal{C}$ is closed for quotients. For each open normal subgroup L of G, we may find an open normal subgroup N of G as in Proposition 1.18 with N closed in L and ${}^{G}\!/_{N} \in \mathcal{C}$, and since ${}^{G}\!/_{L} \cong \left({}^{G}\!/_{N}\right)\left({}^{L}\!/_{N}\right)$, this implies that ${}^{G}\!/_{L} \in \mathcal{C}$. □

We obtain the following important characterization of profinite groups.

Corollary 1.25. *Let $\mathcal{C}$ be the class of all finite groups and G a topological group. The following are equivalent:*

(i) G is profinite

(ii) G is isomorphic, as a topological group, to a closed subgroup of a Cartesian product of finite groups.

(iii) G is compact and $\bigcap\{N \mid N \text{ is an open normal subgroup of } G\} = 1$.

(iv) G is compact and totally disconnected.

The following theorem describes how, given a profinite group G, its subgroups and quotient groups, G can be represented explicitly as inverse limits.

Theorem 1.26. *(i) Let G be a profinite group. If I is a filter base of closed normal subgroups of G, such that $\bigcap_{N\in I} N = 1$, then*

$$G \cong \varprojlim_{N\in I} {}^{G}\!/_{N}$$

Moreover, for each H, K closed in G,

$$H \cong \varprojlim_{N\in I} {}^{H}\!/_{H\cap N}$$

and

$$ {}^{G}\!/_{K} \cong \varprojlim_{N\in I} {}^{G}\!/_{KN}$$

(ii) If $\mathcal{C}$ is a class of finite groups which is closed for subgroups and direct products, then closed subgroups, Cartesian products and inverse limits of pro-$\mathcal{C}$ groups are pro-$\mathcal{C}$ groups. If, in addition, $\mathcal{C}$ is closed for quotients, then quotient groups of pro-$\mathcal{C}$ groups by closed normal subgroups are pro-$\mathcal{C}$ groups.

Proof. (*i*) The first two statements follow directly from Proposition 1.19. The family $J = \{KN \mid N \in I\}$ us a filter base of open normal subgroups of G containing K, and by Lemma 1.2(h) we have

$$\bigcap_{M\in J} M = K \bigcap_{N\in I} N = K$$

Therefore, the third statement follows from Proposition 1.19 aswell.

(ii) The statements about subgroups and quotients follow straight from (i).

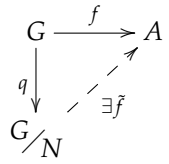
Since closed subgroups of closed groups are closed and the Cartesian products of Cartesian products are Cartesian products, the statements about subgroups follows from the equivalence of (i) and (ii) in 1.24.

Since profinite groups are Hausdorff, 1.13(iii) implies that inverse limits of pro-$\mathcal{C}$ groups are isomorphic to closed subgroups of Cartesian products of pro-$\mathcal{C}$ groups and so, are pro-$\mathcal{C}$ groups.

□

Alternatively, the statement concerning inverse limits of pro-$\mathcal{C}$ groups can be proved directly from the definition of inverse limit

Lemma 1.27. *Let $f: G \longrightarrow A$ be a map from a profinite group G to a discrete space A. Then f is continuous if and only if there exists an open normal subgroup N of G such that f factors through G/N.*



Proof. Clearly, if f factors through G/N, then f is continuous.

Conversely, suppose that f is continuous. Then $\operatorname{Im} f$ is finite. Let $\operatorname{Im} f = \{a_1, \ldots, a_n\}$ and write for each i

$$O_i = \{x \in G \mid f(x) = a_i\}$$

Now, O_i is open, and so is a union of open cosets in G; and O_i is also closed, hence compact, and so is the union of finitely many such cosets Vx. Find an open normal subgroup N which is contained in V for each of the cosets Vx arising. Then each O_i is a union of cosets of N and the result follows. □

Theorem 1.28. *A compact, totally disconnected topological group is profinite.*

Proof. Let G be such a group. Since G is totally disconnected and locally compact, the open subgroups of G form a base of neighborhoods of 1[1]. Such a subgroup U has finite index in G since G is compact; hence its conjugates gUg^{-1}, where $g \in G$ are finite in number and their intersection V is both normal and open in G. Such V's are thus a base of neighborhoods of 1.

The map $G \longrightarrow \varprojlim G/V$ is injective, continuous, and its image is dense; a compactness then shows that it is an isomorphism. Hence G is profinite. □

[1] A proof of this can be found in [2] Chapter III, §3, n°6

Chapter 2

Fundamental Galois Theorem for infinite extensions

Every field k is equipped with a distinguished Galois extension: the separable closure $\overline{k} \mid k$. Its Galois group, $\mathrm{Gal}(\overline{k} \mid k)$ is called the absolute Galois group of k. As a rule, this extension will have infinite degree. There are, of course, some exceptions, which will be characterized in Chapter 3. For example, consider the field $\mathbb{R}^{alg} = \{x \in \mathbb{R} \mid x \text{ is algebraic over } \mathbb{Q}\}$. Then its separable closure (and its algebraic closure) is $\overline{\mathbb{Q}} = \mathbb{R}^{alg}(\sqrt{-1})$. This extension has a finite degree.

For finite field extensions, we can use all the main tools of classical Galois Theory, but, can we do the same for an extension of infinite degree? The answer is no, sadly, and we will see a counterexample:

Consider the absolute Galois group $G := \mathrm{Gal}(\overline{\mathbb{F}}_p \mid \mathbb{F}_p)$ of the field $\mathbb{F}_p$ with p elements. G contains the Frobenius automorphism φ which is given by

$$\varphi(x) = x^p, \quad \text{for all } x \in \overline{\mathbb{F}}_p$$

The subgroup $\langle\varphi\rangle = \{\varphi^n \mid n \in \mathbb{Z}\}$ has the same fixed field $\mathbb{F}_p$ as the whole of G. But contrary to what we are used to in finite Galois theory, we find $\langle\varphi\rangle \subsetneq G$. In order to prove this, let us construct an element $\psi \in G$ which does not belong to $\langle\varphi\rangle$. We choose a sequence $\{a_n\}_{n\in\mathbb{N}}$ of integers satisfying

$$a_n \equiv a_m \pmod{m}$$

whenever $n \mid m$, but such that there is no integer a satisfying $a_n \equiv a \pmod{n}$ for all $n \in \mathbb{N}$. An example of such a sequence is given by $a_n = n' x_n$, where we write $n = n' p^{\nu_p(n)}$, $(n', p) = 1$ and $1 = n' x_n + p^{\nu_p(n)} y_n$, where $\nu_p(n)$ is the p-adic valuation (this will be defined in Chapter 4). Now put

$$\psi_n = \varphi^{a_n}\big|_{\mathbb{F}_{p^n}} \in \mathrm{Gal}(\mathbb{F}_{p^n} \mid \mathbb{F}_p)$$

If $F_{p^m} \subseteq \mathbb{F}_{p^n}$, then $m \mid n$ so that $a_n \equiv a_m \pmod{m}$, and therefore

$$\psi_n\big|_{\mathbb{F}_{p^m}} = \varphi^{a_n}\big|_{\mathbb{F}_{p^m}} = \varphi^{a_m}\big|_{\mathbb{F}_{p^m}} = \psi_m$$

Observe that $\varphi\big|_{\mathbb{F}_{p^m}}$ has order m. Therefore, the ψ_n define an automorphism ψ of $\overline{\mathbb{F}}_p = \cup_{n=1}^{\infty}\mathbb{F}_{p^n}$. Now, ψ can not belong to $\langle\varphi\rangle$ because $\psi = \varphi^a$ for $a \in \mathbb{Z}$ would imply

$$\psi\big|_{\mathbb{F}_{p^n}} = \varphi^{a_n}\big|_{\mathbb{F}_{p^n}} = \varphi^a\big|_{\mathbb{F}_{p^n}}$$

hence $a_n \equiv a \pmod{n}$ for all n, which is what we ruled out by construction.

This might lead us to think that the classical Fundamental Galois Theorem is just wrong in infinite extensions, but we will see that, equipping the Galois group with the correct topology, we can state the Fundamental Galois Theorem for infinite extensions.

2.1 Infinite Galois extensions characterization

Throughout the section we will use the following definitions. Let $K \mid k$ be a (finite or infinite) Galois field extension. Then, we define

$$\mathcal{F} = \{L \mid k \subseteq L \subseteq K, \text{ such that } L \mid k \text{ is a finite Galois extension}\}$$

Also, let

$$\mathcal{N} = \{\mathrm{Gal}(K \mid L) \mid L \in \mathcal{F}\}$$

Now we can define inverse systems indexed by these two sets.

First, in $\mathcal{F}$ we can define a partial ordering $\leq$ such that, for any $L_1, L_2 \in \mathcal{F}$, $L_1 \leq L_2$ if and only if $L_1 \subseteq L_2$. We can also define the continuous maps

$$\begin{array}{rccc} \varphi_{L,L'}: & \mathrm{Gal}(L' \mid k) & \longrightarrow & \mathrm{Gal}(L \mid k) \\ & \sigma & \longmapsto & \sigma\big|_L \end{array}$$

Whenever $L \leq L'$, these maps are well defined (since $L \mid k$ is Galois, hence normal), and satisfy the compatibility condition of the projective systems. Hence, $\big(\mathrm{Gal}(L \mid k), \varphi_{L,L'}\big)_{L\in\mathcal{F}}$ is a projective system.

Before defining the projective system with $\mathcal{N}$, we must prove the following lemma

Lemma 2.1. *Let $K \mid k$ be an infinite Galois extension and let $H \in \mathcal{N}$. Then $H = \mathrm{Gal}(K \mid L)$ is a normal subgroup of $\mathrm{Gal}(K \mid k)$ and $\mathrm{Gal}(L \mid k) \cong {}^{\mathrm{Gal}(K \mid k)}\!/_{\mathrm{Gal}(K \mid L)}$*

Proof. Since $L \mid k$ is a normal extension, the map

$$\begin{array}{rccc} \theta: & \mathrm{Gal}(K \mid k) & \longrightarrow & \mathrm{Gal}(L \mid k) \\ & \sigma & \longmapsto & \sigma\big|_L \end{array}$$

is a well defined map.

Given $\tau \in \mathrm{Gal}(L \mid k)$, τ can be extended to a $\tau' \in \mathrm{Gal}(K \mid k)$ so that $\tau'\big|_L = \tau$, thus, θ is surjective.

Since $\mathrm{Ker}(\theta) = \mathrm{Gal}(K \mid E) = H$, H is a normal subgroup of G and by the first isomorphism theorem, $\mathrm{Gal}(E \mid k) \cong {}^{\mathrm{Gal}(K \mid k)}\!/_{\mathrm{Gal}(K \mid L)}$. □

We can now define a projective system indexed by $\mathcal{N}$. We define a partial ordering on $\mathcal{N}$, $\leq$, such that, if $H_1, H_2 \in \mathcal{N}$, then $H_1 \leq H_2$ if and only if $H_2 \subseteq H_1$. We can also define the continuous homomorphisms

$$\begin{array}{rccc} \varphi_{H,H'}: & \mathrm{Gal}(K \mid k)/H' & \longrightarrow & \mathrm{Gal}(K \mid k)/H \\ & \sigma H' & \longmapsto & \sigma H \end{array}$$

We know from the Lemma that H is a normal subgroup of $\mathrm{Gal}(K \mid k)$, so the quotients are well defined and if $H \leq H'$, the map $\varphi_{H,H'}$ is a well defined continuous homomorphism. Hence, $\left(\mathrm{Gal}(K \mid k)/H, \varphi_{H,H'}\right)_{H \in \mathcal{N}}$ is an inverse system.

However, these two systems are the same one since, by the lemma, $\mathrm{Gal}(K \mid k)/\mathrm{Gal}(K \mid L) \cong \mathrm{Gal}(L \mid k)$. Also, if $H = \mathrm{Gal}(L \mid k)$, $H' = \mathrm{Gal}(L' \mid k)$, with $H, H' \in \mathcal{N}$, we have $H \leq H'$ if and only if $L \leq L'$. Finally, the two maps $\varphi_{L,L'}$ and $\varphi_{H,H'}$ correspond to each other exactly, which proves the equality between the inverse systems we stated.

This equality will give us the freedom to jump from one inverse system to the other when necessary.

Remark 2.2. The projective system $\left(\mathrm{Gal}(K \mid k)/H, \varphi_{H,H'}\right)_{H \in \mathcal{N}}$ gives a collection of homomorphisms

$$\begin{array}{rccc} \varphi_H: & \mathrm{Gal}(K \mid k) & \longrightarrow & \mathrm{Gal}(K \mid k)/H \\ & \sigma & \longmapsto & \sigma H \end{array}$$

which are compatible with the maps $\varphi_{H,H'}$. Then, by the universal property of projective limits, there is a unique homomorphism $\chi': \mathrm{Gal}(K \mid k) \longrightarrow \varprojlim_{H \in \mathcal{N}} \mathrm{Gal}(K \mid k)/H$ and since $\varprojlim_{H \in \mathcal{N}} \mathrm{Gal}(K \mid k)/H \cong \varprojlim_{E \in \mathcal{F}} \mathrm{Gal}(E \mid k)$, we also have a homomorphism $\chi: \mathrm{Gal}(K \mid k) \longrightarrow \varprojlim_{E \in \mathcal{F}} \mathrm{Gal}(E \mid k)$

Lemma 2.3. *Let $\alpha_1, \ldots, \alpha_n \in K$. Then there is an $E \in \mathcal{F}$ such that $\alpha_1, \ldots, \alpha_n \in E$*

Proof. Let $k \subseteq E \subseteq K$ be the splitting field of $\prod_{i=1}^{n} \mathrm{Irr}(\alpha_i, k)$. Clearly, E is normal over k and since $E \subseteq K$ and $K \mid k$ is separable then $E \mid k$ is separable. Hence, $E \mid k$ is Galois. Finally, $[E : k] \leq \prod_{i=1}^{n} \deg(\mathrm{Irr}(\alpha_i, k)) < \infty$, so $E \in \mathcal{F}$. □

Corollary 2.4.

$$\bigcup_{E \in \mathcal{F}} E = K$$

Proof. Let $x \in K$. Then, there exists $E \in \mathcal{F}$ such that $x \in E \subseteq \bigcup_{E \in \mathcal{F}} E$.

Since $E \subseteq K$ for each $E \in \mathcal{F}$, $\bigcup_{E \in \mathcal{F}} E \subseteq K$. □

Notation. *If G is a group, we will denote the identity element in G as 1_G when we have multiple groups.*

Proposition 2.5. *The homomorphism* $\chi : \operatorname{Gal}(K \mid k) \longrightarrow \varprojlim_{E\in\mathcal{F}} \operatorname{Gal}(E \mid k)$ *is an isomorphism.*

Proof. First note that the uniqueness of χ implies that it is the map $\sigma \longmapsto (\sigma\big|_E)_{E\in\mathcal{F}}$, since this map is a compatible homomorphism.

χ is injective, because $\chi(\sigma) = (1_E)_{E\in\mathcal{F}}$ implies that $\sigma_E = 1_E$ for every $E \in \mathcal{F}$. However, since $K = \bigcup_{E\in\mathcal{F}} E$, one has that $\sigma = 1_K$.

Finally, χ is surjective. Let $(\sigma_E)_{E\in\mathcal{F}} \in \varprojlim_{E\in\mathcal{F}} \operatorname{Gal}(E \mid k)$. Let us define σ as follows. Let $\alpha \in K$, so there exists some $E \in \mathcal{F}$ such that $\alpha \in E$ by Lemma 2.3. Then let $\sigma(\alpha) = \sigma_E(\alpha)$ for such E. In this way, one defines σ for each $\alpha \in K$ and thus obtains $\sigma \in \operatorname{Gal}(K \mid k)$. Since $E_1 \leq E_2$ if and only if $\operatorname{Gal}(E_1 \mid k) \leq \operatorname{Gal}(E_2 \mid k)$, if $\alpha \in E_1 \leq E_2$, then $\sigma_{E_1}(\alpha) = \sigma_{E_2}(\alpha)$, so σ is well defined. Then, $\chi(\sigma) = (\sigma_E)_{E\in\mathcal{F}}$ so χ is surjective. □

Corollary 2.6. *For any infinite Galois extension* $K \mid k$, $\operatorname{Gal}(K \mid k)$ *is profinite. Hence,* $\operatorname{Gal}(K \mid k)$ *is compact, Hausdorff and totally disconnected.*

We have now equipped $\operatorname{Gal}(K \mid k)$ with a topology. We will now define a different topology on $\operatorname{Gal}(K \mid k)$ called the Krull topology. This topology might seem a bit more workable, but we shall see that it is really nothing more that the topology we have just defined.

The Krull Topology

Lemma 2.7.

$$\bigcap_{H\in\mathcal{N}} H = 1$$

Proof. Since $\operatorname{Gal}(K \mid k)$ is profinite and by Lemma 2.1, any $H \in \mathcal{N}$ is normal in $\operatorname{Gal}(K \mid k)$, by Corollary 1.25 (iii), we have the result. □

Corollary 2.8. *For all* $\sigma \in \operatorname{Gal}(K \mid k)$,

$$\bigcap_{H\in\mathcal{N}} \sigma H = \{\sigma\}$$

Notation. *We denote the fixed field of an extension* $K \mid k$ *by* H*, a subgroup of the Galois group, as* K^H.

Lemma 2.9. *If* $H_1, H_2 \in \mathcal{N}$ *then* $H_1 \cap H_2 \in \mathcal{N}$.

Proof. Let $H_1 = \operatorname{Gal}(K \mid E_1)$ and $H_2 = \operatorname{Gal}(K \mid E_2)$, for $E_1, E_2 \in \mathcal{F}$. Because E_1, E_2 are finite Galois over k, so is E_1E_2, so $E_1E_2 \in \mathcal{F}$. However, $\operatorname{Gal}(K \mid E_1E_2) = H_1 \cap H_2$ because:

$$\sigma \in H_1 \cap H_2 \iff \sigma\big|_{E_1} = 1_{E_1} \text{ and } \sigma\big|_{E_2} = 1_{E_2} \iff E_1, E_2 \in K^{\langle\sigma\rangle} \iff$$
$$\iff E_1E_2 \in K^{\langle\sigma\rangle} \iff \sigma \in \operatorname{Gal}(K \mid E_1E_2)$$

Hence, $H_1 \cap H_2 = \operatorname{Gal}(K \mid E_1E_2) \in \mathcal{N}$. □

Lemma 2.10. *$\mathcal{B} = \{\sigma H \mid \sigma \in \mathrm{Gal}(K \mid k),\ H \in \mathcal{N}\}$ forms a basis for a topology on $\mathrm{Gal}(K \mid k)$.*

Proof. Each open set is a union of cosets σH hence an arbitrary union of open sets is also a union of such cosets, so in this topology an arbitrary union of open sets is open.

$\mathrm{Gal}(K \mid k)$ is open because $k \mid k$ is a finite extension of degree 1. The main thing to check is that open sets are closed under finite intersections. It suffices to check this for two elements of the basis, which we do now. If τH_1 and τH_2 are two basis elements, let $\tau \in \tau_1 H_1 \cap \tau_2 H_2$. Then $\tau H_1 = \tau_1 H_1$ and $\tau H_2 = \tau_2 H_2$, so $\tau(H_1 \cap H_2) = \tau H_1 \cap \tau H_2 = \tau_1 H_1 \cap \tau_2 H_2$. Lemma 2.9 implies that $H_1 \cap H_2 \in \mathcal{N}$, hence $\tau(H_1 \cap H_2)$ is open. Finally, for some $H \in \mathcal{N}$ with $H \neq G$, choose $\tau_1, \tau_2 \in G$ such that $\tau_1 H \neq \tau_2 H$. Then, $\tau_1 H \cap \tau_2 H = \emptyset$ and $\emptyset$ is open, so $\mathcal{B}$ is indeed the basis for a topology on G. □

In light of this lemma, we define

Definition 2.11. *Let $K \mid k$ be a Galois extension. The Krull topology on $\mathrm{Gal}(K \mid k)$ is the topology with basis all cosets σH, where $\sigma \in \mathrm{Gal}(K \mid k)$, $H = \mathrm{Gal}(K \mid E)$ and $E \mid k$ is a finite Galois extension.*

Remark 2.12. If $H \in \mathcal{N}$, with $H = \mathrm{Gal}(K \mid E)$, by Lemma 2.1 we know that $\mathrm{Gal}(E \mid k) \cong {}^{\mathrm{Gal}(K \mid k)}\!/_{\mathrm{Gal}(K \mid E)}$, so $[G : H]$ is finite. Thus, there exists $\sigma_1, \sigma_2, \ldots, \sigma_n$ such that

$$G = H \cup \sigma_1 H \cup \cdots \cup \sigma_2 H$$

So $G \setminus H$ is also a union of open sets. Therefore H is both open and closed. Thus, the Krull topology has a basis of subgroups which are both closed and open.

Proposition 2.13. *Giving $\mathrm{Gal}(K \mid k)$ the Krull topology and $\varprojlim_{E \in \mathcal{F}} \mathrm{Gal}(E \mid k)$ the profinite group topology, the map $\chi : \mathrm{Gal}(K \mid k) \longrightarrow \varprojlim_{E \in \mathcal{F}} \mathrm{Gal}(E \mid k)$ is a homeomorphism of topological spaces.*

Proof. We already know that χ is a group isomorphism by Proposition 2.5, so χ is bijective. The open sets in $\mathrm{Gal}(K \mid k)$ are generated by the basis $\{\sigma H \mid \sigma \in \mathrm{Gal}(K \mid k),\ H \in \mathcal{N}\}$ and by the sub-basis $\bigcup_{E \in \mathcal{F}} \{\pi_E^{-1}(\{\sigma\}) \mid \sigma \in \mathrm{Gal}(E \mid k)\}$ in $\varprojlim_{E \in \mathcal{F}} \mathrm{Gal}(E \mid k)$. First, let us check that χ is continuous. $\chi^{-1}(\pi_E^{-1}(\{\sigma\})) = \{\tau \in \mathrm{Gal}(K \mid k) \mid \tau\big|_E = \sigma\} = \{\tau \in \mathrm{Gal}(K \mid k) \mid \tau \text{ is an extension of } \sigma \text{ to } K\} = \bigcup_{\tau \in \mathrm{Gal}(K|k)} \tau\,\mathrm{Gal}(K \mid E)$ where the union is taken over all such τ which extend σ, and which is clearly open in G by definition of the Krull topology.

Now, let us check that χ^{-1} is continuous, which is equivalent to checking that χ is an open map. Let σH be a basic open set for the Krull topology on $\mathrm{Gal}(K \mid k)$, so $\sigma \in \mathrm{Gal}(K \mid k)$ and $H = \mathrm{Gal}(K \mid E)$ for some $E \in \mathcal{F}$. Then $\chi(\sigma H) = \{(\sigma\tau_L)_{L \in \mathcal{F}} \mid \tau_{L|E} = 1_{L \cap E}\} = \{(\tau_L)_{L \in \mathcal{F}} \mid \sigma^{-1}\tau_{L|E} = 1_{L \cap E}\} = \{(\tau_L)_{L \in \mathcal{F}} \mid \tau_{L|E} = \sigma_{L \cap E}\} = \pi^{-1}(\{\sigma\big|_E\})$ which is also open in $\varprojlim_{E \in \mathcal{F}} \mathrm{Gal}(E \mid k)$. Thus χ is a homeomorphism. □

Corollary 2.14. *Equipped with the Krull topology, the Galois group of an infinite algebraic extension $K \mid k$ forms a topological group. That is, the map from $\mathrm{Gal}(K \mid k) \times \mathrm{Gal}(K \mid k)$ to $\mathrm{Gal}(K \mid k)$ such that $(x, y) \longmapsto xy^{-1}$ is continuous under the Krull topology.*

Corollary 2.15. *Equipped with the Krull topology, the Galois group of an algebraic extension is compact, Hausdorff and totally disconnected.*

2.2 Fundamental Galois Theorem for infinite extensions

We are on the brink of proving the fundamental theorem for infinite extensions. Before that, we will require one more lemma.

Lemma 2.16. *Let $K \mid k$ be a Galois extension, $G = \mathrm{Gal}(K \mid k)$, H closed subgroup of G and let $H = \mathrm{Gal}(K \mid L)$ where $L = K^H$. Then $H' = \overline{H}$, where $\overline{H}$ denotes the closure of H in the Krull topology on G.*

Proof. Since every element on H fixes L by definition of L, we have that H is a closed subgroup of H'. Now take $\sigma \in G \setminus H'$. Then, there is an $\alpha \in L$ with $\sigma(\alpha) \neq \alpha$. Choose $E \in \mathcal{F}$ with $\alpha \in E$ (which we know we can do by Lemma 2.3) and let $N = \mathrm{Gal}(K \mid E)$. Then, for any $\tau \in N$, $\tau(\alpha) = \alpha$, so $\sigma\tau(\alpha) = \sigma(\alpha) \neq \alpha$. Hence, σN is an open neighborhood of σ disjoint from H', so $G \setminus H'$ is open and hence H' is closed.

Finally, we want to show that $H' \subseteq \overline{H}$. Then we will have $H \subseteq H' \subseteq \overline{H}$ and H' is closed, so $H' = \overline{H}$. Let $\sigma \in H'$ and again, choose any $N \in \mathcal{N}$, $N = \mathrm{Gal}(K \mid E)$ with $E \in \mathcal{F}$. Let $H_0 = \{\rho_E \mid \rho \in H\}$. This is a subgroup of $\mathrm{Gal}(E \mid k)$, where $\mathrm{Gal}(E \mid k)$ is finite. Since the fixed field of H_0 is $K^H \cap E$, that is, $L \cap E$. The classical fundamental theorem shows that $H_0 = \mathrm{Gal}(E \mid E \cap L)$. Since $\sigma \in H'$, $\sigma\big|_L = 1_L$, so $\sigma\big|_L \in H_0$. Thus there is $\rho \in H$ with $\rho\big|_E = \sigma\big|_E$ and thus $\sigma^{-1}\rho \in \mathrm{Gal}(K \mid E) = N$ so $\rho \in \sigma N \cap H$. Thus, for every $\sigma \in H'$ and every basic open neighborhood σN of σ, we have $(\sigma N \cap H') \setminus \{\sigma\} \neq \emptyset$, so $\sigma \in \overline{H}$. Therefore, we have $H' \subseteq \overline{H}$, so $H' = \overline{H}$. □

Now, finally, we are ready to state and prove the generalized fundamental theorem, valid for all infinite Galois extensions.

Theorem 2.17 (Fundamental Theorem of Infinite Galois Theory)**.** *Let K be a Galois extension of k, and let $G = \mathrm{Gal}(K \mid k)$.*

(1) With the Krull topology on G, the maps $E \longmapsto \mathrm{Gal}(K \mid E)$ and $H \longmapsto K^H$ give and inclusion-reversing correspondence between intermediate fields $k \subseteq E \subseteq K$ and closed subgroups H of G.

(2) If E corresponds to H, then the following are equivalent:

- *(i)* $[G : H] < \infty$.
- *(ii)* $[E : k] < \infty$.
- *(iii) H is open.*

(3) If the conditions in (2) are satisfied, then $[G : H] = [E : k]$.

(4) For any closed subgroup H of G, where $H = \mathrm{Gal}(K \mid E)$, we have that H is normal in G if and only if $E \mid k$ is Galois. If this is the case, then there exists a group isomorphism $\theta : {}^{G}\!/_{H} \longrightarrow \mathrm{Gal}(E \mid k)$.

Proof. (1) If $k \subseteq E \subseteq K$ (not necessarily $E \mid k$ in $\mathcal{F}$), then $K \mid E$ is normal and separable, hence Galois. Thus E is the fixed field of $\mathrm{Gal}(K \mid E)$. If H is a closed subgroup of G, then Lemma 2.16 shows that $\mathrm{Gal}(K \mid K^H) = \overline{K}$. Thus, we have that $H = \mathrm{Gal}(K \mid E)$ for some $k \subseteq E \subseteq K$ if and only if H is closed, so the maps $L \longmapsto \mathrm{Gal}(K \mid L)$ and $H \longmapsto K^H$ give the desired correspondence between intermediate fields and closed subgroups.

(2)

$(i) \Rightarrow (iii)$ Let $k \subseteq E \subseteq K$, $H = \mathrm{Gal}(K \mid E)$ and suppose that $[G : H] < \infty$. Then $G \setminus H$ is a finite union of closed cosets (because H is closed) so H is open.

$(iii) \Rightarrow (ii)$ Now, if $H = \mathrm{Gal}(K \mid E)$ is open then H contains some basic open neighborhoods of 1, so $N \subseteq H$ for some $N \in \mathcal{N}$. If $L = K^N$, then $E \subseteq L$, $L \in \mathcal{F}$, so $[L : k] < \infty$ and $[L : k] = [L : E][E : k] < \infty$ implies $[E : k] < \infty$.

$(ii) \Rightarrow (i)$ If $[E : k] < \infty$, then choose $L \in \mathcal{F}$ with $E \subseteq L$ (which can always be done by Lemma 2.3), and let $N = \mathrm{Gal}(K \mid L)$. Then N is a closed subgroup of H since $E \subseteq L$ so $[G : H] \leq [G : N] < \infty$.

(3) We know that $|\mathrm{Gal}(E \mid k)| = [E : k]$, thus $[G : H] = [E : k]$.

(4) Suppose that H normal subgroup of G is closed in G, so $H = \mathrm{Gal}(K \mid E)$. Let $\alpha \in E$ and let $f(X) = \mathrm{Irr}(\alpha, k)(X)$. If $\beta \in K$ is another root of f, then there is $\sigma \in G$ with $\sigma(\alpha) = \beta$. If $\tau \in H$, then $\tau(\beta) = \sigma^{-1}(\sigma\tau\sigma^{-1}(\alpha)) = \sigma^{-1}(\alpha) = \beta$, since $\sigma\tau\sigma^{-1} \in H$. Thus, β is in the fixed field of H which is E, so f splits over E. Thus, $E \mid F$ is normal, $E \mid k$ is separable since $K \mid k$ is, so $E \mid k$ is Galois.

Conversely, if $E \mid k$ is Galois, then the map $\theta : \quad G \longrightarrow \mathrm{Gal}(E \mid k)$ such that $\theta(\sigma) = \sigma\big|_E$ is well defined (since $E \mid k$ is normal), and $\mathrm{Ker}\,\theta = \mathrm{Gal}(K \mid E) = H$, which is normal in G. θ is also surjective by the isomorphism extension theorem, so $G/H \cong \mathrm{Gal}(E \mid k)$.

□

Remark 2.18. If $K \mid k$ is a finite Galois extension, then the Krull topology on $\mathrm{Gal}(K \mid k)$ is discrete. This is because $K \mid k$ is finite, hence $\mathrm{Gal}(K \mid K) = \{1\}$ is open. Thus, every subgroup of $\mathrm{Gal}(K \mid k)$ is closed, so we obtain our original bijective correspondence given by the classical fundamental Galois theorem.

2.3 Profinite groups as Galois groups

To finish off this chapter, we are going to include a result that characterizes all profinite groups as Galois groups of an algebraic field extension.

Lemma 2.19. *Let θ be an homomorphism from a profinite group G to the Galois group of an algebraic field extension $K \mid k$ (the continuity of θ is not assumed). For each $x \in K$, write G_x for the group of elements of G whose images under θ fix x. Suppose that G_x is open for each x and that the subfield fixed by $\theta(G)$ is k. Then $K \mid k$ is a Galois extension, and θ is continuous and surjective.*

Proof. Write R_x for the intersection of the conjugates of G_x in G, for each $x \in K$. Since G_x is open, it contains an open normal subgroup, and so R_x is open.

Let $x_1, \ldots, x_r \in K$ and write L for the subfield generated by k and all images of $x_1, \ldots, x_r$ under the elements of $\theta(G)$. Thus, G induces automorphisms of L and if $g \in G$, then $\theta(g)$ fixes each element of L if and only if g lies in the open normal subgroup $R_{x_1} \cap \cdots \cap R_{x_r}$. It follows that the image of G in $\mathrm{Gal}(L \mid k)$ is finite and that its fixed field is k. A result of Artin in classical Galois theory asserts that if H is a finite group of automorphisms of a field F and if the fixed field is F_0, then the extension $F \mid F_0$ is Galois and $H = \mathrm{Gal}(F \mid F_0)$. It follows that $L \mid k$ is a finite Galois extension and that G maps onto $\mathrm{Gal}(L \mid k)$.

Now K is a union of such fields L, and so, the extension $K \mid k$ is Galois. The image of $\theta(G)$ in $\mathrm{Gal}(L \mid k)$ under the map from $\mathrm{Gal}(K \mid k)$ to $\mathrm{Gal}(L \mid k)$ is $\mathrm{Gal}(L \mid k)$; since this map has kernel $\mathrm{Gal}(K \mid L)$ it follows that

$$\mathrm{Gal}(K \mid k) = {}^{\theta(G)}\!/_{\mathrm{Gal}(K \mid L)}$$

for each L. Each subgroup $\theta^{-1}(\mathrm{Gal}(K \mid L))$ is open and so, since the subgroups $\mathrm{Gal}(K \mid L)$ form a base of neighborhoods of 1 in $\mathrm{Gal}(K \mid k)$, the map θ is continuous. Therefore $\theta(G)$ is closed in $\mathrm{Gal}(K \mid k)$, and from Lemma 1.2(h) we conclude that θ is surjective. □

Theorem 2.20. *Every profinite group G is isomorphic, as a topological group, to a Galois group.*

Proof. Let F be an arbitrary field. Write S for the disjoint union of the sets ${}^{G}\!/_{N}$, where N is an open normal subgroup of G, and let $K = F(X_s \mid s \in S)$, where the elements X_s are independent transcendentals over F in bijective correspondence with the elements of S. The natural action of F on S as a group of permutations induces a homomorphism θ from G to the group of field automorphisms of K. If $u \in K$, then we have $u \in F(X_{s_1}, \ldots, X_{s_r})$, say; and if $s_i = N_i g_i$ for $i = 1, \ldots, r$ then (in the notation of Lemma 2.19) we have $N_1 \cap \cdots \cap N_r$ closed subgroup of G_u, which is open.

Let k be the fixed field of G. The map $\theta : G \longrightarrow \mathrm{Gal}(K \mid k)$ is clearly and injective homomorphism, and from Lemma 2.19 it is continuous and surjective. We conclude that θ is an homeomorphism, since G is compact and $\mathrm{Gal}(K \mid k)$ is Hausdorff, hence θ is an isomorphism of profinite groups. □

This concludes the most theory-heavy part of this work.

We recall that we have already shown an example of an infinite Galois group, the absolute Galois group of the Galois extension $\mathrm{Gal}(\overline{\mathbb{F}_p} \mid \mathbb{F}_p) = \widehat{\mathbb{Z}}$ in Section 1.2.1. In general, these groups are very difficult to compute, so this is why there are not a lot of examples that we can easily explain.

We are now going to characterize the dimension of the absolute Galois group $\mathrm{Gal}(\overline{k} \mid k)$ using the Artin-Schreier theorem and we are going to explore the p-adics integers $\mathbb{Q}_p$ and its algebraic extensions briefly.

Chapter 3

Algebraic closure characterization

3.1 Formally Real Fields

Definition 3.1. *A field F is said to be ordered if there is a given subset P in F such that P is closed under addition and multiplication and*

$$F = P \sqcup \{0\} \sqcup -P$$

where $-P = \{-p \mid p \in P\}$.

Remark 3.2. We can prove that $\mathbb{Q}$ is an ordered field, taking $P = \{x \in \mathbb{Q} \mid x > 0\}$.

Remark 3.3. An ordered field F is said to be totally ordered if we define $a > b$ to mean $a - b \in P$. Moreover, if $a > b$, then $a + c > b + c$ for every $c \in F$, and $ap > bp$ for every $p \in P$.

Lemma 3.4. *If F is a totally ordered field, then $1 \in P$ and for every $x \in F$, such that $x \neq 0$, $x^2 > 0$.*

Proof. Since $1 \neq 0$, we have either $1 \in P$ or $1 \in -P$. By definition, $1 \in -P$ implies $-1 \in P$, but, $(-1)(-1) = (-1)^2 = 1$, by the second assertion, hence, P would not be closed under multiplication. Therefore, $1 \in P$.

Now, let us prove that for any $x \in F \setminus \{0\}$, $x^2 > 0$. If $x > 0$, then $x^2 = x \cdot x > x \cdot 0 = 0$. If $x < 0$, then $-x > 0$, so $x^2 = (-x) \cdot (-x) > (-x) \cdot 0 = 0$. □

Proposition 3.5. *If F is totally ordered, then -1 is not a sum of squares in F.*

Proof. First of all, let us reduce the problem to a simpler one. Suppose

$$-1 = \sum_{a_i \in F} a_i^2$$

Since $1 \in F$ and $1^2 = 1$, we can rewrite the expression as

$$0 = \sum_{a_i \in F} a_i^2 + 1 = \sum_{a_i \in F} a_i^2$$

Now, for each $a \neq 0$, $a^2 = (-a)^2 > 0$

Hence, $\sum a_i^2 = 0$ only if $a_i = 0$, for each i. □

Corollary 3.6. *The characteristic of a totally ordered field is always 0*

Definition 3.7. *A field F is called formally real if -1 is not a sum of squares in F.*

Remark 3.8. If F is a totally ordered field, F is formally real.

Lemma 3.9. *Let P_0 be a subgroup of F^* of a field F such that P_0 is closed under addition and contains all non-zero squares. Let $a \in F^*$ such that $-a \notin P_0$. Then $P_1 = P_0 + P_0 a = \{b + ca \mid b, c \in P_0\}$ is a subgroup of F^* closed under addition.*

Proof. Evidently, P_1 is closed under addition; if $b, c, b', c' \in P_0$ such that $b + ca, b' + c'a \in P_1$, then $(b + ca) + (b' + c'a) = (b + b') + (c + c')a$, and since P_0 is closed under addition, $(b + b'), (c + c') \in P_0$. It is also closed under multiplication, since $(b + ca)(b' + c'a) = (bb' + cc'a^2) + (bc' + b'c)a$ and $bb' + cc'a^2, bc + b'c \in P_0$.

We note that $0 \notin P_1$, otherwise, we would have $0 = b + ca$, which gives $-a = bc^{-1} \in P_0$.

Also, we have $(b + ca)^{-1} = (b + ca)(b + ca)^{-2} = b(b + ca)^{-2} + c(b + ca)^{-2}a \in P_1$ since $(b + ca)^{-2} = ((b + ca)^{-1})^2 \in P_0$ is a non-zero square.

Hence, P_1 is a subgroup of F^*. □

Theorem 3.10. *A field F can be ordered by a subset P if and only if it is formally real.*

Proof. The implication to the right has been discussed in Remark 3.8.

Conversely, let F be formally real and let $P_0 = \{\sum a_i^2 \mid a_i \neq 0\}$. P_0 is closed under addition, and since $\left(\sum a_i^2\right)\left(\sum b_j^2\right) = \sum a_i^2 b_j^2$, P_0 is closed under multiplication.

Moreover, P_0 contains all of the non-zero squares. Hence, if $a = \sum a_i^2$, $a_i \neq 0$, then $a^{-1} = aa^{-2} \in P_0$.

Thus, P_0 satisfies the conditions of Lemma 3.9 and so, the set of subsets P_1 satisfying these conditions is not empty. We can apply Zorn's lemma to conclude that this set of subsets of F contains a maximal element P. It follows from the Lemma that if $a \in F^*$, then either $a \in P$ or $-a \in P$. Hence, $F = P \cup \{0\} \cup -P$, where $-P = \{-p \mid p \in P\}$. Since $0 \notin P$ and P is closed under addition, $P \cap -P = \emptyset$. Thus P, $-P$ and $\{0\}$ are disjoint and since P is closed under addition and multiplication, P gives an ordering of the field F. □

Definition 3.11. *A field R is called real closed if it is ordered and if*

(i) Every positive element of R has a square root in R.

(ii) Every polynomial of odd degree in $R[X]$ has a root in R.

Proposition 3.12. *The ordering in a real closed field R is unique and any automorphism of such field is an order-automorphism.*

The proof for this can be found on [5] Chapter 5, §1 (Theorem 5.1).

Proposition 3.13. *If R is real closed, then $R(\sqrt{-1})$ is algebraically closed.*

The proof for this can be found on [5] Chapter 5, §1 (Theorem 5.2).

Lemma 3.14. *If F is formally real, then any extension field $F(r)$ is formally real if either $r = \sqrt{a}$ for $a \in F$, $a > 0$, or r is algebraic over F with minimum polynomial of odd degree.*

Proof. First, let $r = \sqrt{a}$, $a > 0$. Suppose that $F(r)$ is not formally real. Then $r \notin F$ and we have $\{a_i\}, \{b_i\} \in F$ such that $-1 = \sum(a_i + b_i r)^2$. This gives $\sum a_i^2 + \sum b_i^2 a = -1$. Since $a > 0$, this is impossible.

In the second case, let $f(x)$ be the minimum polynomial of r. Then the degree of $f(x)$ is odd. We shall use induction on $m = \deg(f(x))$. Suppose that $F(r)$ is not formally real. Then we have polynomials $g_i(x)$ of degree less than m such that $\sum g_i(r)^2 = -1$. Hence, we have

$$\sum g_i(x)^2 = -1 + f(X)g(X) \tag{3.1}$$

where $g(X) \in F[X]$. Since F is formally real and the leading coefficient of $g_i(X)^2$ is a square, it follows that $\deg(-1 + f(X)g(X)) = \deg(\sum g_i(X)^2)$ is even and less that $2m$. It follows that $\deg(g(X))$ is odd and less than m. Now, $g(X)$ has an irreducible factor $h(X)$ of odd degree. Let s be a root of $h(X)$ and consider $F(s)$. By the other induction hypothesis, this is formally real. On the other hand, substitution of s in the equation 3.1, yields the contradiction $\sum g_i(s)^2 = -1$. □

Theorem 3.15. *A field R is real closed if and only if R is formally real and no proper algebraic extension of R is formally real.*

Proof. Suppose that R is real closed. Then $C = R(\sqrt{-1})$ is algebraically closed and $R \subsetneq C$. Evidently C is an algebraic closure of R and so, any algebraic extension of R can be regarded as a subfield of $C \mid R$. Hence, if it is a proper extension it must be C, which is not formally real since it contains $\sqrt{-1}$.

Conversely, suppose that R is formally real and no proper algebraic extension of R has this property. Let $a \in R$ be positive. Then Lemma 3.14 show that $R(\sqrt{a})$ is formally real. Hence, $R(\sqrt{a}) = R$ and $\sqrt{a} \in R$.

Next, let $f(x)$ be a polynomial of odd degree with coefficients in R. Let $g(x)$ be an irreducible factor of $f(x)$ of odd degree and consider an extension field $R(r)$ where $g(r) = 0$. By Lemma 3.14, $R(r)$ is formally real. Hence, $R(r) = R$. Then $r \in R$ and $f(r) = 0$. We have therefore verified the two defining propertied of a real closed field. Hence, R is real closed. □

Theorem 3.16. *A field R is real closed if and only if $\sqrt{-1} \notin R$ and $C = R(\sqrt{-1})$ is algebraically closed*

Proof. It suffices to show that if R has the stated properties, then R is real closed. Suppose that R satisfies the conditions. We show first that the sum of two squares in R is a square. Let $a, b \in R \setminus \{0\}$ and let u be an element of C such that $u^2 = a + b\sqrt{-1}$. We have the automorphism $x + y\sqrt{-1} \longmapsto x - y\sqrt{-1}$ of $C \mid R$ whose set of fixed points is R. Now,

$$a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1}) = u^2\overline{u^2} = (u\overline{u})^2$$

and $u\overline{u} \in R$. Thus $a^2 + b^2$ is a square in R. By induction, every sum of squares in R is a square. Since -1 is not a square in R, it is not a sum of squares and hence, R is formally real. On the other hand, since C is algebraically closed, the first part of the proof of Theorem 3.15 shows that no proper algebraic extension of R is real closed. Hence R is real closed by Theorem 3.15. □

3.2 Real Closures

Even if this section is not used in the proof of the Artin-Schreier theorem, it has an important theorem that only requires a bit more of work.

Definition 3.17. *Let F be an ordered field. An extension field of F is called a real closure of F if*

(i) R is real closed and algebraic over F

(ii) The (unique) order in R is an extension of the given order in F.

Definition 3.18. *A Strum chain or Strum sequence of a square free polynomial p for the closed interval $[a, b]$ is a finite sequence of polynomials $p_0, p_1, \ldots, p_m$ of decreasing degree with the following properties*

(SC1) $p_0(a)p_0(b) \neq 0$

(SC2) If $p(c) = 0$ for $c \in [a, b]$ then there exist open intervals (c_1, c) and (c, c_2) such that $p_0(u)p_1(u) < 0$ for any $u \in (c_1, c)$ and $f_0f_1(u) > 0$ for any $u \in (c, c_2)$.

(SC3) If $p_i(\xi) = 0$ for $0 < i < m$, then $\operatorname{sign}(p_{i-1}(\xi)) = -\operatorname{sign}(p_{i+1}(\xi))$.

(SC4) p_m has no roots in $[a, b]$.

Theorem 3.19 (Strum's Theorem)**.** *Let R be a real closed field, $p_0, \ldots, p_m$ be a Strum chain of the square free polynomial p and let $\sigma(\xi)$ denote the number of sign changes, ignoring zeros, in the sequence*

$$p_0(\xi), p_1(\xi), \ldots, p_m(\xi)$$

Now, if $a, b \in R$, with $a < b$, the number of distinct roots of p in the half open interval $(a, b]$ is $\sigma(a) - \sigma(b)$.

Lemma 3.20. *Let R be a real closed field and $f(X) \in R[X]$ such that $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Let us define $M = 1 + |a_1| + \cdots + |a_n|$, where $|\cdot|$ denotes the absolute value in R. Then, every root of $f(X)$ in R lies in the interval $(-M, M)$*

A proof of Strum's theorem and the Lemma can be found on [5] Chapter 5, §2.

Lemma 3.21. *Let R_1, R_2 be two real closed fields, F_i a subfield of R_i, $a \longmapsto \overline{a}$ an order-isomorphism of F_1 onto F_2, where the order in F_i is the one induced from R_i.*

Suppose that $f(X)$ is a monic polynomial in $F_1[X]$, $\overline{f}(X)$ the corresponding polynomial in $F_2[X]$. Then $f(X)$ has the same number of roots in R_1 as $\overline{f}(X)$ has in R_2.

Proof. Defining M as above, the first number of roots is $\sigma(-M) - \sigma(M)$ and the second is $\sigma(-\overline{M}) - \sigma(\overline{M})$. Since $a \longmapsto \overline{a}$ is an order isomorphism, $\sigma(-M) - \sigma(M) = \sigma(-\overline{M}) - \sigma(\overline{M})$. □

Theorem 3.22. *Any ordered field has a real closure.*

If F_1 and F_2 are ordered fields with real closures R_1 and R_2 respectively, then, any order isomorphism of F_1 into F_2 has a unique extension to an isomorphism of R_1 onto R_2 and this extension preserves order.

Proof. Let F be an ordered field and let $\overline{F}$ be an algebraic closure of F. Let $\overline{F} \mid E$ be a subfield such that

$$E = F(\{\sqrt{a} \mid a > 0,\ a \in F\})$$

Now, E is formally real. Otherwise, E contains elements a_i such that $\sum a_i^2 = -1$.

The a_i are contained in a subfield generated over F by a finite number of square roots of positive elements of F, lets call it $G = F(\sqrt{b_1}, \ldots, \sqrt{b_r})$. Now, since F is formally real, $F(\sqrt{b_1})$ is formally real by Lemma 3.14. Since $F(\sqrt{b_1})$ is formally real, $F(\sqrt{b_1})(\sqrt{b_2}) = F(\sqrt{b_1}, \sqrt{b_2})$ is formally real by Lemma 3.14. Repeating this process, we get that G is formally real. Now, since $a_i \in G$ and G is formally real, it contradicts the assumption that E contains a_i such that $\sum a_i^2 = -1$.

Let $\mathcal{F} = \{E \mid E \text{ is formally real and } E \subseteq \overline{F}\}$. This set is not empty and by Zorn's Lemma, we have a maximal subfield R in the set. We claim that R is real closed.

If not, there exists a proper algebraic extension R' of R that is formally real by Theorem 3.15. Since $\overline{F}$ is an algebraic closure of R, we may assume that $R' \subseteq \overline{F}$ so, we have $R \subsetneq R' \subseteq \overline{F}$. This contradicts the maximality of R. Hence, R is real closed.

Now, let $a \in F$ and $a > 0$. Then $a = b^2$ for some $b \in E \subseteq R$, hence $a > 0$ in the order defined in R. Thus, the order in R is an extension of that of F and hence R is a real closure of F.

Let F_1 and F_2 be ordered fields and R_i a real closure of F_i. Let

$$\begin{array}{rccc} \sigma: & F_1 & \longrightarrow & F_2 \\ & a & \longmapsto & \overline{a} \end{array}$$

be an order isomorphism of F_1 onto F_2. We would like to show that σ can be extended to an isomorphism

$$\begin{array}{rccc} \Sigma: & R_1 & \longrightarrow & R_2 \\ & a & \longmapsto & \overline{a} \end{array}$$

Let $r \in R_1$, $g(X) = \mathrm{Irr}(r, F_1)$ and $r_1 < r_2 < \cdots < r_k = r < \ldots r_m$ be the roots of $g(X)$ in R_1.

By the Lemma 3.21, the polynomial $\overline{g}(X)$ has precisely m roots in R_2 arranged as $\overline{r_1} < \cdots < \overline{r_m}$. We define

$$\begin{array}{rccc} \Sigma: & R_1 & \longrightarrow & R_2 \\ & r_k & \longmapsto & \overline{r_k} \end{array}$$

It is a bijective map and $\Sigma\big|_{F_1} = \sigma$. Let us show that Σ is an isomorphism. To see this, we show that if S is any finite subset of R_1, there exists a subfield E_1 of $R_1 \mid F_1$ and a monomorphism

$$\eta: \quad E_1 \mid F_1 \longrightarrow R_2 \mid F_2$$

that extends σ and preserves the order of the elements of S. That is, if $S = \{s_1 < \cdots < s_n\}$, then $\eta s_1 < \cdots < \eta s_n$. Let $T = S \cup \{\sqrt{s_{i+1} - s_i} \mid 1 \leq i \leq n-1\}$ and let $E_1 = F_1(T)$. Evidently, E_1 is finite dimensional over F_1 and so, by the primitive element theorem, there exists $\omega \in E_1$ such that $E_1 = F_1(\omega)$. Let $f(X) = \mathrm{Irr}(\omega, F_1)$. By the Lemma 3.21, $\overline{f}(X)$ has a root $\overline{\omega}$ in R_2, and we have a monomorphism

$$\begin{array}{rccc} \eta: & E_1 \mid F_1 & \longrightarrow & E_2 \mid F_2 \\ & \omega & \longmapsto & \overline{\omega} \end{array}$$

Now, $\eta(s_{i+1}) - \eta(s_i) = \eta((\sqrt{s_{i+1} - s_i})^2) = (\eta(\sqrt{s_{i+1} - s_i}))^2 > 0$. Hence, η preserves the order of S.

Let r and s be any two elements of E_1 and apply the result to the finite set S consisting of the roots of $\mathrm{Irr}(r, F_1)$, $\mathrm{Irr}(s, F_1)$, $\mathrm{Irr}(r+s, F_1)$ and $\mathrm{Irr}(sr, F_1)$.

Since η preserves the order of the elements of S, $\eta(r) = \Sigma(r)$, $\eta(s) = \Sigma(s)$, $\eta(s+r) = \Sigma(r+s)$ and $\eta(rs) = \Sigma(rs)$. Hence,

$$\Sigma(r+s) = \eta(r+s) = \eta(r) + \eta(s) = \Sigma(r) + \Sigma(s)$$

and

$$\Sigma(rs) = \eta(rs) = \eta(r)\eta(s) = \Sigma(r)\Sigma(s)$$

Thus Σ is a morphism and, more accurately, and isomorphism.

It remains to show that Σ is unique and is order preserving. Let Σ' be an isomorphism of R_1 onto R_2. Since Σ' maps squares intro squares and the subsets of positive elements of the R_i are sets of non-zero squares, it is clear that Σ' preserves order. Suppose also that Σ' is an extension of σ. Then it is clear from the definition of Σ that $\Sigma' = \Sigma$. □

Corollary 3.23. *If R_1 and R_2 are two real closures of an ordered field F, then the identity map on F can be extended in a unique manner to an order isomorphism of R_1 onto R_2. In this sense, there is a unique real closure of F.*

Remark 3.24. The field $\mathbb{R}^{alg} = \{x \in \mathbb{R} \mid x \text{ is algebraic over } \mathbb{Q}\}$ is the real closure of $\mathbb{Q}$ and its called the field of real algebraic numbers.

The field $\overline{\mathbb{Q}} = \mathbb{R}^{alg}(\sqrt{-1})$ is the algebraic closure of $\mathbb{Q}$. This is the field of algebraic numbers.

3.3 Artin-Schreier Theorem

The Artin-Schreier Theorem states the following,

Theorem. *Let C be an algebraically closed field with F a subfield such that $1 < [C : F] < \infty$. Then $C = F(i)$ and F is a real closed field.*

To prove this theorem, we will need some previous lemmas to simplify the proof.

Some results on Traces and Norms

Let $E \mid F$ be finite Galois, $G = \text{Gal}(E \mid F) = \{\eta_1 = 1, \eta_2, \ldots, \eta_n\}$. If $u \in E$, we define

$$T_{E|F}(u) = \sum_{i=1}^{n} \eta_i(u), \qquad N_{E|F}(u) = \prod i = 1^n \eta_i(u)$$

We consider some familiarity with traces and norms, so we are going to enunciate and prove the theorems directly.

Theorem 3.25. *Let $E \mid F$ be a finite dimensional Galois extension and G its Galois group. Let $\eta \longmapsto u_\eta$ be the map from G into the multiplicative group E^* satisfying the equations*

$$u_{\zeta\eta} = \zeta(u_\eta)u_\zeta$$

for every $\eta, \zeta \in G$. Then, there exists a non-zero $v \in E$ such that

$$u_\eta = v(\eta(v))^{-1}$$

Proof. Since $u_\eta \neq 0$ and the automorphism $\eta \in G$ are linearly independent over E, there exists an element $w \in E$ such that

$$v = \sum_{\eta \in G} u_\eta \eta(w) \neq 0$$

Then for $\zeta \in G$, we have

$$\begin{aligned} \zeta(v) &= \textstyle\sum_\eta \zeta(u_\eta)(\zeta\eta)(w) \\ &= \textstyle\sum_e tau_{\zeta\eta}u_\zeta^{-1}(\zeta\eta)(w) \\ &= \left(\textstyle\sum_z etau_{\zeta\eta}(\zeta\eta)(w)\right) u_\zeta^{-1} \\ &= \left(\textstyle\sum_e tau_\eta\eta(w)\right) u_\zeta^{-1} \\ &= vu_\zeta^{-1} \end{aligned}$$

Hence $u_\zeta = v(\zeta(v))^{-1}$ as required. □

Lemma 3.26. *Let E be a cyclic extension of the field F, η a generator of the cyclic Galois group of $E \mid F$. Then $N_{E|F}(u) = 1$ for some $u \in E$ if and only if there exists a $v \in E$ such that $u = v(\eta(v))^{-1}$.*

Proof. If we suppose $u \in E$ satisfies $N_{E|F}(u) = 1$, we can define

$$u_{\eta^i} = u\eta(u)\eta^2(u)\dots\eta^{i-1}(u), \qquad 1 \leq i \leq n$$

Then for $i + j \leq n$, $u_{\eta^j}\eta^j(u_{\eta^i}) = u\eta(u)\cdots\eta^{j-1}(u)\eta^j(u)\cdots\eta^{i+j-1}(u) = u_{\eta^{i+j}}$. The same relation holds for $i + j > n$ since $u_1 = u_{\eta^n} = N(u) = 1$. Thus, the equations in Theorem 3.25 are satisfied for $G = \langle\eta\rangle$. Hence, there exists a v such that $u = u_\eta = v(\eta(v))^{-1}$.

Conversely, if $u = v(\eta(v))^{-1}$, then

$$N_{E|F}(u) = N_{E|F}(v)N_{E|F}(\eta(v)^{-1}) = N_{E|F}(v)N_{E|F}(v)^{-1} = 1$$

□

This theorem and lemma have additive analogues that are proved in a similar manner. Therefore we are not going to prove them, but one may find this proofs on Chapter 4, §15 of [5].

Theorem 3.27. *Let $E \mid F$ be a finite Galois extension and let $G = \mathrm{Gal}(E \mid F)$. Let $\eta \longmapsto d_n$ be a map of G into E satisfying*

$$d_{\zeta\eta} = d_\zeta + \zeta(d_\eta)$$

for every $\eta, \zeta \in G$. Then there exists a $c \in E$ such that

$$d_\eta = c - \eta(c), \quad \eta \in G$$

Lemma 3.28. *Let $E \mid F$ be a cyclic Galois extension with Galois groups $G = \langle\eta\rangle$. Let d be an element of E of trace 0. Then there exists a $c \in E$ such that $d = c - \eta(c)$.*

Theorem 3.29. *Let F contain n distinct nth roots of unity and let $E \mid F$ be an n-dimensional cyclic Galois extension of F. Then $E = F(u)$, where $u^n \in F$.*

Proof. Let z be a primitive nth root of unity. We have $N_{E|F} = z^n = 1$. Hence, by Lemma 3.26, there exists $u \in E$ such that $z = u(\eta(z))^{-1}$, where η is the generator of the Galois group. Then we have $\eta(u) = z^{-1}u$ and $\eta(u^n) = \eta(u)^n = (z^{-1}u)^n = u^n$. Accordingly, $u^n \in F$. Also, $\eta(u) = z^{-1}u$ gives $\eta^i(u) = z^{-i}u$ and shows that there are n distinct elements in the orbit of u under $\mathrm{Gal}(E \mid F)$. Hence, the minimum polynomial of u over F has degree n and $E = F(u)$. □

Theorem 3.30. *Let F be a field of characteristic $p \neq 0$ and let $E \mid F$ be a p-dimensional cyclic extension of F. Then $E = F(c)$ where $c^p - c \in F$.*

Proof. We have $T_{E|F}(1) = \sum_{i=1}^{p} \eta_i(1) = \sum_{i=1}^{p} 1 = 0$. Hence, by Lemma 3.28, we have an element $c \in E$ such that $\eta(c) = c + 1$. Then $\eta^i(c) = c + i$ and the orbit of c under $\mathrm{Gal}(E \mid F)$ contains p elements. Hence $E = F(c)$. Also, $\eta(c^p - c) = \eta(c)^p - \eta(c) = (c+1)^p - (c+1) = c^p - c$. Hence, $c^p - c \in F$. □

Now that we have finished with the results concerning norms and traces, let us use them in order to prove the following lemmas

Lemma 3.31. *Let F be a field of characteristic $p > 0$ and let a not a pth power. Then for any $e \geq 1$, the polynomial $X^{p^e} - a$ is irreducible in $F[X]$.*

Proof. If E is the splitting field of $X^{p^e} - a$, then we have the factorization

$$X^{p^e} - a = (X - r)^{p^e}$$

in $E[X]$, with $r^{p^e} = a$. Hence, if $g(X)$ is a monic factor of X^{p^e} in $F[X]$, then $g(X) = (X - r)^k$, with $k = \deg(g(X))$. Then $r^k \in F$ and $r^{p^e} = a \in F$. If $p^f = (p^e, k)$ there exist integers m, n such that

$$p^f = mp^e + nk$$

Then $r^{p^f} = (r^{p^e})^m (r^k)^n \in F$. If $k < p^e$, then $f < e$ and if $b = r^{p^f}$, then $b^{p^{e-f}} = a$, contrary to the hypothesis that a is not a pth power in F. □

Lemma 3.32. *If F is a field of characteristic p and $a \in F$ is not of the form $u^p - u$, with $u \in F$, then $X^p - X - a$ is irreducible in $F[X]$*

Proof. If r is a root of $X^p - X - a$ in $C[X]$, where C is the splitting field of this polynomial, then $r + 1, r + 2, \ldots r + (p - 1)$ are also roots of $X^p - X - a$. Hence

$$X^p - X - a = \prod_{i=0}^{p-1} (X - (r + i))$$

is a factorization in $C[X]$.

If $g(X) = X^k - bX^{k-1} + \ldots$ is a factor of $X^p - X - a$ in $F[X]$, then $b = kr + l$, where l is an integer. Hence, $k < p$ implies $r \in F$. Since $r^p - r = a$, this contradicts the hypothesis. □

Lemma 3.33. *Let F be a field of characteristic p. If $C \mid F$ is a splitting field of $X^p - X - a$, where $a \neq u^p - u$, with $u \in F$, there exists a field $C' \mid C$ such that $[C' : C] = p$.*

Proof. If r is a root of $X^p - X - a$ in C, then $r, r + 1, \ldots, r + (p - 1)$ are also roots of $X^p - X - a$ in C. Therefore, $C = F(r)$ and we have the relation

$$r^p = r + a \tag{1}$$

We claim that $ar^{p-1} \in C$ is not of the form $u^p - u$, $u \in C$. To prove it, we can write any $u \in C$ as $u_0 + u_1 r + \cdots + u_{p-1} r^{p-1}$, with $u_i \in F$, since $\{1, r, \ldots, r^{p-1}\}$ is an F-basis of C. The condition $u^p - u = ar^{p-1}$ and (1) give

$$u_0^p + u_1^p (r+a) + \cdots + u_{p-1}^p (r+a)^{p-1} - u_0 - u_1 r - \cdots - u_{p-1} r^{p-1} = ar^{p-1}$$

This can be rewritten as the system of equations

$$\begin{aligned} u_0^p - u_0 + u_1^p a + u_2^p a^2 + \cdots + u_{p-1}^p a^{p-1} &= 0 \\ \vdots & \\ u_{p-1}^p - u_{p-1} &= a \end{aligned}$$

Where the ith line corresponds to the coefficients of r^{i-1}.

This yields $u_{p-1}^p - u_{p-1} = a$, contrary to the hypothesis on a. It now follows from Lemma 3.32 that $X^p - X - ar^{p-1}$ is irreducible in $C[X]$. Hence, if C' is the splitting field over C of this polynomial, then $[C' : C] = p$ □

Theorem 3.34. *Let C be an algebraically closed field with F a subfield such that $1 < [C : F] < \infty$. Then $C = F(i)$ and F is a real closed field.*

Proof. We will prove that $C = F(i)$ and the result will follow from Theorem 3.16.

We would like to first prove that $C \mid F$ is Galois. Since C is algebraically closed, then $C \mid F$ is clearly normal.

Now let us see that $C \mid F$ is separable. As a matter of fact, we will prove that F is a perfect field hence $C \mid F$ separable. If F has characteristic 0, it is already perfect, so let us suppose the characteristic of F is $l > 0$. Now, we'd like to prove $F = F^l$. Suppose there exists an element $a \in F$ such that $a \notin F^l$. Then, by 3.31, $X^{l^m} - a$ is irreducible for each $m \geq 1$. Hence, we can build extensions over F of degree l^m, for each $m \geq 1$. Since this number tends to infinity and $[C : F] < \infty$, this leads to contradiction.

The next step is to prove that $[C : F] = 2$ and that ζ_4, a primitive 4th root of unity, is not in F. Let

$$G := \mathrm{Gal}(C \mid F)$$

so $[C : F] = \mid G \mid$. If $|G| > 2$, then $|G|$ is divisible by an odd prime or 4. Hence, by the first Sylow theorem, G has a subgroup H of order an odd prime or 4. Now, let

$$K := C^H$$

We note that $[C : K] = |H|$, therefore, if we prove that $|H| = 2$, this suffices to prove that $|G| = 2$.

Assume $[C : K] = p$ a prime. Since $H = \mathrm{Gal}(C \mid K)$, H is a cyclic subgroup of G, therefore let σ be a generator of H. We'd like to show that $p = 2$.

The first step is to show that the characteristic of K can not be p. Suppose it is. Then, $C = K(r)$ by Theorem 3.30, where r is a root of the irreducible polynomial $X^p - X - a$. By

Lemma 3.33, since C is the splitting field of $X^p - X - a$, there exists a field $C' \mid C$ such that $[C' : C] = p$, but this contradicts the fact that C is algebraically closed.

Since C is algebraically closed of characteristic different from p, C contains a root of unity of order p, call it ζ. Now, since $[F(\zeta) : F] \leq p - 1$ and $[C : F] = p$, we must have $[F(\zeta) : F] = 1$, so $\zeta \in F$. This means $C \mid F$ is cyclic of degree p with F containing a pth root of unity, so, by Theorem 3.29, $C = F(\gamma)$, where $\gamma^p \in F$.

Choose $\beta \in C$ such that $\beta^p = \gamma$, so $\beta^{p^2} = \gamma^p \in F$. Thus, $\beta^{p^2} = \sigma(\beta^{p^2}) = \sigma(\beta)^{p^2}$, hence $\sigma(\beta) = \omega\beta$, with $\omega^{p^2} = 1$. Thus, ω^p is a pth root of unity, so $\omega^p \in F$.

Now, if $\omega^p = 1$, then $\sigma(\beta^p) = \sigma(\beta)^p = \beta^p$, hence $\beta^p \in F$. But $\beta^p = \gamma$ and $\gamma \notin F$. Thus, $\omega^p \neq 1$, so ω has order p^2 and ω^p has order p.

Now, $\sigma(\omega) = \omega^a$, for some a prime with p. Hence,

$$\omega^p = \sigma(\omega^p) = \omega^{ap} = (\omega^p)^a$$

This implies $a \equiv 1 \pmod{p}$, hence $a = 1 + kp$, for some $k \in \mathbb{Z}$. Therefore,

$$\sigma(\omega) = \omega^{1+kp}$$

From the equation $\sigma(\beta) = \omega\beta$, we get

$$\beta = \sigma^p(\beta) = \omega\sigma(\omega)\cdots\sigma^{p-1}(\omega)\beta = \omega^{1+(1+pk)+\cdots+(1+pk)^{p-1}}\beta,$$

so we get the sequence of congruences

$$\begin{aligned}
1 + (1+pk) + \cdots + (1+pk)^{p-1} &\equiv 0 \pmod{p^2} \\
\sum_{i=0}^{p-1} (1+pk)^i &\equiv 0 \pmod{p^2} \\
p + \frac{p(p-1)}{2}pk &\equiv 0 \pmod{p^2} \\
1 + \frac{p(p-1)}{2}k &\equiv 0 \pmod{p} \\
\frac{p(p-1)}{2}k &\equiv p-1 \pmod{p} \\
\frac{p}{2}k &\equiv 1 \pmod{p}
\end{aligned}$$

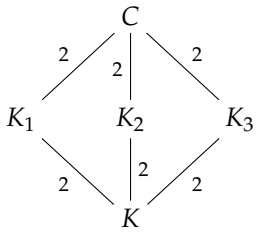
Now, for $\frac{p}{2}$ to be a valid integer, we can either have an even k, but that leads to $\frac{p}{2}k \equiv 0 \pmod{p}$, or $p = 2$. Then

$$k \equiv 1 \pmod{2}$$

implies that k is odd. Therefore, ω has order $p^2 = 4$ and $\sigma(\omega) = \omega^{1+pk} = \omega^{1+2k} = \omega^3$, since we can not have $\sigma(\omega) = \omega$. Now, $\omega^2 = -1$ and $\omega = i$. Thus, if $[C : K]$ is prime, then it equals 2, C does not have characteristic 2 and $i \notin F$.

If $[C : K] = 4$, then H can be either C_4 or $C_2 \times C_2$. In both cases, H has a subgroup of order 2, so there is an intermediate field $K \subset K' \subset C$ with $[C : K]$. Since 2 is prime, we can repeat all the argument above and that implies $i \notin K'$, hence, $i \notin K$. Now, $K(i)$ is a subfield of C with $[C : F(i)] = 2$ and $F(i)$ contains i. This yields a contradiction in both cases, $H \cong C_4$ and $H \cong C_2 \times C_2$.

If $H \cong C_4$, this is clear, since C_4 has a unique subgroup of order 2, hence $F(i) = K'$.
If $H \cong C_2 \times C_2$, we have the following extension diagram



In this case, $K' = K_j$, for every $j = 1, 2, 3$. This implies $i \notin K_j$, for each $j = 1, 2, 3$. Now, $K(i) = K_j$ for some $j = 1, 2, 3$ and this also yields the contradiction.

Hence, if F is non-algebraically closed field whose algebraic closure C is a finite extension, then $[C : F] = 2$ and $C = F(i)$. □

Chapter 4

The p-adic numbers

The goal for this chapter is to construct an extension of $\mathbb{Z}_p$ which is a complete space and also algebraically closed, in the same sense as it is done in $\mathbb{Z}$, where we complete $\mathbb{Q}$ to $\mathbb{R}$ and then we compute its algebraic closure, $\mathbb{C}$.

However, there are differences with the real case: We will define $\mathbb{Z}_p$ and we will complete it to $\mathbb{Q}_p$. When we compute its algebraic closure, $\overline{\mathbb{Q}}_p$, we will see that this field is not complete, so we will have to complete it again. Luckily, this process does not go on, the completion of $\overline{\mathbb{Q}}_p$, $\mathbb{C}_p$, is a field which is complete and algebraically closed.

4.1 The p-adic metric space

Definition 4.1. *Let p be any prime number. For any non-zero integer a, let the p-adic ordinal of a, denoted by $\operatorname{ord}_p a$ be the highest power of p which divides a. That is, $a \equiv 0 \pmod{p^{\operatorname{ord}_p a}}$, but $a \not\equiv 0 \pmod{p^{\operatorname{ord}_p a+1}}$. If $a = 0$, we define $\operatorname{ord}_p a = \infty$ for any p.*

Remark 4.2. $\operatorname{ord}_p(a_1 a_2) = \operatorname{ord}_p(a_1) + \operatorname{ord}_p(a_2)$

Definition 4.3. *For $a, b \in \mathbb{Z}$, $\operatorname{ord}_p(\frac{a}{b}) = \operatorname{ord}_p(a) - \operatorname{ord}_p(b)$*

Notation. *This p-adic ordinal is more commonly written as the function $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$, called the p-adic exponential valuation. We will refer to it this way from now on.*

Proposition 4.4. *The map $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$ such that $|x|_p = \frac{1}{p^{v_p(x)}}$ if $x \neq 0$ and $|0|_p = 0$ is a norm. We call it the p-adic norm.*

Definition 4.5. *A norm is called non-Archimedean if $\|x + y\| \leq \max\{\|x\|, \|y\|\}$ always holds.*
A norm which is not non-Archimedean is called Archimedean.

Remark 4.6. The absolute value in $\mathbb{Q}$, $|\cdot|$, is an Archimedean norm.
The p-adic norm, $|\cdot|_p$, is non-Archimedean

Notation. *The absolute value is also called the infinity norm $|\cdot|_\infty$.*

Theorem 4.7 (Ostrowski)**.** *Every non-trivial norm $\|\cdot\|$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p or $p = \infty$.*

Remark 4.8. The theorem states that if $\|\cdot\|$ is non-Archimedean, then $\|\cdot\|$ is equivalent to $|\cdot|_p$ for some prime p and if it is Archimedean, then $\|\cdot\|$ is equivalent to $|\cdot|_\infty$.

Since we perfectly know how Archimedean norms work, let us have an insight on how one might grasp a non-Archimedean distance.

Let F be a field and $\|\cdot\|$ a non-Archimedean metric. The triangle inequality here is $|x-y| \leq \max\{\|x\|, \|y\|\}$. Now, suppose $\|x\| \leq \|y\|$. Then,

$$\|x-y\| \leq \|y\|$$

but we also have

$$\|y\| = \|x-(x-y)\| \leq \max\{\|x\|, \|x-y\|\}, \text{ hence, } \|y\| \leq \|x-y\|$$

Therefore, $\|y\| = \|x-y\|$. This implies that, if we have a triangle with two sides of different lengths ($\|x\|$, $\|y\|$), then the third one is forced to be as long as the longer one of those two. This implies that every triangle is isosceles in a non-Archimedean metric.

This result should not come as a surprise, since if we think of the case $|\cdot|_p$ over $\mathbb{Q}$, if two natural numbers are divisible by two different powers of p, then their difference is divisible by precisely the lower power of p.

We call the principle $\|x-y\| \leq \max\{\|x\|, \|y\|\}$, with the equality holding if $\|x\| \neq \|y\|$, the isosceles triangle principle.

As a second example, let $\|\cdot\|$ be a non-Archimedean norm. Define $D(a,r)^{\circ} = \{x \in F \mid \|x-a\| < r\}$. Then, every point of $D(a,r)^{\circ}$ is a center, i.e. for any $b \in D(a,r)^{\circ}$, $D(a,r)^{\circ} = D(b,r)^{\circ}$. The proof of this fact is simple enough:

If $x \in D(a,r)^{\circ}$, then $\|x-a\| < r$. $\|x-b\| = \|(x-a)+(a-b)\| \leq \max\{\|x-a\|, \|a-b\|\} < r$. Hence, $x \in D(b,r)^{\circ}$.

Now, if $x \in D(b,r)^{\circ}$, then $\|x-b\| < r$. $\|x-a\| = \|(x-b)+(b-a)\| \leq \max(\|x-b\|, \|b-a\|) < r$. Hence, $x \in D(a,r)^{\circ}$.

We also note that with the relation $\leq$ instead of $<$, the proof works equally, hence, the fact is satisfied with the closure of $D(a,r)^{\circ}$.

After this brief exploration of non-Archimedean distances, let us continue with our main goal: the definition of the p-adic metric space.

Definition 4.9. *The metric space $(\mathbb{Q}, |\cdot|_p)$ is called the p-adic metric space*

Proposition 4.10. *For every rational number $a \neq 0$, one has*

$$\prod_p |a|_p = 1$$

where p varies over all prime numbers as well as the symbol ∞.

Proof. In the prime factorization

$$a = \pm \prod_{p \neq \infty} p^{\nu_p}$$

of a, the exponent ν_p of p is precisely the p-adic exponential valuation $v_p(a)$ and the sign equals $\frac{a}{|a|_\infty}$. The equation therefore reads

$$a = \frac{a}{|a|_\infty} \prod_{p \neq \infty} \frac{1}{|a|_p}$$

so that one has indeed $\prod_p |a|_p = 1$. □

Having introduced the p-adic absolute value $|\cdot|_p$ on the field $\mathbb{Q}$, let us now give the definition of the field $\mathbb{Q}_p$ of p-adic numbers, imitating the analytic construction of the real numbers.

4.2 The field of p-adic numbers $\mathbb{Q}_p$

Definition 4.11. *A Cauchy sequence in a metric space $(F, \|\cdot\|)$ is by definition a sequence $\{x_n\}$ of elements of F, such that for every $\varepsilon > 0$, there exists a positive integer n_0 satisfying*

$$\|x_n - x_m\| < \varepsilon, \text{ for all } n, m \geq n_0$$

Let p be a fixed prime number and let S be the set of Cauchy sequences $\{a_i\}$ of rational numbers. We call two sequences $\{a_i\}, \{b_i\} \in S$ equivalent if $|a_i - b_i|_p$ tends to zero. Then we define

$$\mathbb{Q}_p = S/\sim$$

where $\sim$ is the equivalence relation defined above.

For any $x \in \mathbb{Q}$, let $\{x\}$ denote the constant Cauchy sequence of all terms equal to x. $\{x\} \sim \{x'\}$ if and only if $x = x'$, hence, we denote each constant sequence $\{x\} \in \mathbb{Q}_p$ as x.

We extend the norm $|\cdot|_p$ on $\mathbb{Q}_p$ as $|\{a_i\}|_p = \lim_{i\to\infty} |a_i|_p$. This is well defined since the limit always exists: If $a_i = 0$ for every i, then obviously $|\{0\}|_p = \lim |0|_p = 0$ and if $a \in S \setminus \{0\}$, then for some $\varepsilon > 0$ and for all $N > 0$, there exists $i_n > N$ with $|a_{i_N}|_p > \epsilon$.

If we choose a large enough N such that $|a_i - a_j| < \varepsilon$ for every $i, j > N$, then $|a_i - a_{i_N}|_p < \varepsilon$, for every $i > N$. And since $|\cdot|_p$ is non-Archimedean, we have

$$|a_i - a_{i_N}| < \varepsilon \iff |a_i|_p = |a_{i_N}|_p$$

Thus, for all $i > N$, $|a_i|_p$ has the constant value $|a_{i_N}|_p$. This is then, $\lim_{i\to\infty} |a_i|_p$.

Now we will define addition, multiplication and its respective inverses and identity elements. For each definition, we will have to show that it is, in fact, a Cauchy sequence and also that it is well defined, in the sense that it does not depend on the class representative. This will be done for addition only, since the other ones are similar.

- Addition in $\mathbb{Q}_p$. Let $\{a_i\}, \{b_i\} \in \mathbb{Q}_p$. We define the sum $\{a_i\} + \{b_i\}$ as the sequence of the element-wise sum, $\{a_i + b_i\}$.

First, let us check that $\{a_i + b_i\}$ is a Cauchy sequence.

$$|a_i + b_i - a_j - b_j|_p = |(a_i - a_j) + (b_i - b_j)|_p \leq \max\{|a_i - a_j|_p, |b_i - b_j|_p\}$$

Now, since $\{a_i\}, \{b_i\} \in \mathbb{Q}_p$, they are Cauchy sequences, hence, for each $\varepsilon > 0$, there exists integers N_a, N_b such that $|a_i - a_j| < \varepsilon$, $\forall\, i, j \geq N_a$ and $|b_i - b_j| < \varepsilon$, $\forall\, i, j \geq N_b$. Taking $N = \max\{N_a, N_b\}$, we have, for all $i, j \geq N$,

$$|a_i + b_i - a_j - b_j| < \varepsilon$$

Now let us show that is well defined. Let $\{a_i'\}, \{b_i'\} \in S$ such that $\{a_i'\} \sim \{a_i\}$ and $\{b_i'\} \sim \{b_i\}$. We would like to see $\{a_i + b_i\} \sim \{a_i' + b_i'\}$.

$$|a_i + b_i - a_i' + b_i'|_p = |(a_i - a_i') + (b_i - b_i')|_p \leq \max\{|a_i - a_i'|, |b_i - b_i'|\}$$

Since $\{a_i\} \sim \{a_i'\}$, $|a_i - a_i'|_p \to 0$ as $i \to \infty$ and since $\{b_i\} \sim \{b_i'\}$, $|b_i - b_i'|_p \to 0$ as $i \to \infty$. Hence, $|a_i + b_i - a_i' + b_i'|_p \to 0$ as $i \to \infty$.

- Additive identity element in $\mathbb{Q}_p$. We define the additive identity element in $\mathbb{Q}_p$ as the constant series $\{0\}$.
- Additive inverses in $\mathbb{Q}_p$. Let $\{a_i\} \in \mathbb{Q}_p$. Then we define the additive inverse $-\{a_i\}$ as the sequence $\{-a_i\}$, which is obviously the additive inverse, since $\{a_i\} + \{-a_i\} = \{a_i - a_i\} = \{0\}$.
- Multiplication in $\mathbb{Q}_p$. Let $\{a_i\}, \{b_i\} \in \mathbb{Q}_p$. We define multiplication in $\mathbb{Q}_p$ as $\{a_i\}\{b_i\} = \{a_i b_i\}$.
- Multiplicative identity element. We define the multiplication identity element in $\mathbb{Q}_p$ as the constant series $\{1\}$.
- Multiplicative inverse in $\mathbb{Q}_p$. Let $\{a_i\} \in \mathbb{Q}_p$. We define the multiplicative inverse of $\{a_i\}$, $\{a_i\}^{-1}$ as $\{a_i^{-1}\}$. We will prove that this does not suppose any problem, because we can always change the class representative to be one with $a_i \neq 0$ for every i.

Lemma 4.12. *Every Cauchy sequence in S is equivalent to another one which has $a_i \neq 0$, for every i.*

Proof. Let $\{a_i\} \in S$ be an arbitrary Cauchy sequence. We would like to show that $\{a_i\} \sim \{a_i'\}$, where $a_i' = a_i$, if $a_i \neq 0$ and $a_i' = p^i$, if $a_i = 0$. Let us define the subsequence $\{a_{i_k}\}_{k \in I}$ of $\{a_i\}$ such that $a_{i_k} = 0$, for each $k \in I$ and $a_i \neq 0$ if $i \in \mathbb{N} \setminus I$.

Suppose that $\#I < \infty$. Then, there exists $N = \max I$ and clearly $|a_i - a_i'|_p \to 0$ as $i \to \infty$.

Suppose now that $\#I = \infty$. Notice that, $\forall \varepsilon > 0$ $|a_i - a_i'|_p = 0 < \varepsilon$ if $i \notin I$. Hence, the choice of N relies on the $i \in I$. Since $|a_i - a_i'|_p = |p^i|_p = p^{-i}$ and since $\lim_{i \in I} p^{-i} = 0$, $\forall \varepsilon > 0$, there exists $N > 0$ such that $|a_i - a_i'|_p < \varepsilon$ for every $i \geq N$. □

Proposition 4.13. *$\mathbb{Q}_p$ is a field*

We only have to prove all the field axioms. It is easy, since every one of them follows from the respective axiom over $\mathbb{Q}$.

Finally, we shall prove that $\mathbb{Q}_p$ is complete under $|\cdot|_p$.

Theorem 4.14. *$\mathbb{Q}_p$ is complete under $|\cdot|_p$*

Proof. If $\{a_j\}_{j\in\mathbb{N}}$ is a sequence of equivalence classes which is Cauchy in $\mathbb{Q}_p$, then for each a_j we take a representative Cauchy sequence of $\mathbb{Q}$, $\{a_{j_i}\}_{i\in\mathbb{N}}$, where, for each j we have $|a_{j_i} - a_{j_k}|_p < p^j$, whenever $i, k \geq N_j$. We would like to show $\lim_{j\to\infty} a_j = \{a_{i_{N_i}}\}$. That is,

$$|a_j - \{a_{i_{N_i}}\}|_p < \varepsilon, \quad \forall j > N$$

We note that $a_j - \{a_{i_{N_i}}\}$ is a subtraction in $\mathbb{Q}_p$, which we have defined earlier as taking representatives for each class and subtracting them. For $\{a_{i_{N_i}}\}$ it is clear which representative we shall take. For a_j, let us take $\{a_{j_i}\}$, the same representative Cauchy sequence of $\mathbb{Q}$ we picked before.

Now, $a_j - \{a_{i_{N_i}}\}$ is the Cauchy sequence $\{a_{j_i} - a_{j_{N_j}}\}$, but $|a_{j_i} - a_{j_{N_j}}|_p < p^{-j}$, for all $i > N_j$. Therefore, $\forall\varepsilon > 0$, there is a j such that $|a_{j_i} - a_{j_{N_j}}|_p < p^{-j} < \varepsilon$, for all $i \geq N_j$. Hence, $\{a_j\}_{j\in\mathbb{N}}$ converges to $\{a_{i_{N_i}}\}$. □

Proposition 4.15. *The set*

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

is a subring of $\mathbb{Q}_p$. It is the closure with respect to $|\cdot|_p$ of the ring $\mathbb{Z}$ in the field $\mathbb{Q}_p$.

Proof. That $\mathbb{Z}_p$ is closed under addition and multiplication follows from

$$|x + y|_p \leq \max\{|x|_p, |y|_p\} \quad \text{and} \quad |xy|_p = |x|_p|y|_p$$

If $\{x_n\}$ is a Cauchy sequence in $\mathbb{Z}$ and $x = \lim_{n\to\infty} x_n$, then $|x_n|_p \leq 1$ implies also $|x|_p \leq 1$, hence $x \in \mathbb{Z}_p$. Conversely, let $x = \lim_{n\to\infty} x_n \in \mathbb{Z}_p$, for a Cauchy sequence $\{x_n\}$ in $\mathbb{Q}$. We saw above that one has $|x|_p = |x_n|_p \leq 1$, for $n \geq n_o$, i.e. $x_n = \frac{a_n}{b_n}$, with $a_n, b_n \in \mathbb{Z}$, $(b_n, p) = 1$. Choosing for each $n \geq n_0$ a solution $y_n \in \mathbb{Z}$ of the congruence $b_n y_n \equiv a_n \pmod{p^n}$ yields $|x_n - y_n|_p \leq p^{-n}$, and hence $x = \lim_{n\to\infty} y_n$, so that x belongs to the closure of $\mathbb{Z}$. □

The group of units of $\mathbb{Z}_p$ is obviously

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$$

Every element $x \in \mathbb{Q}_p^*$ admits a unique representation

$$x = p^m u \quad \text{with } m \in \mathbb{Z} \text{ and } u \in \mathbb{Z}_p^*$$

for if $v_p(x) = m \in \mathbb{Z}$, then $v_p(xp^{-m}) = 0$, hence, $|xp^{-m}|_p = 1$, i.e. $u = xp^{-m} \in \mathbb{Z}_p^*$.

Having defined $\mathbb{Z}_p$ in this manner, we would like to show that this is the $\mathbb{Z}_p$ that we constructed with the profinite limit $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

Proposition 4.16. *The nonzero ideals of the ring $\mathbb{Z}_p$ are the principal ideals*

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq n\}$$

with $n \geq 0$ and one has

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

Proof. Let $\mathfrak{a} \neq (0)$ be an ideal of $\mathbb{Z}_p$ and $x = p^m u$, $u \in \mathbb{Z}_p^*$, an element of $\mathfrak{a}$ with smallest possible m (since $|x|_p \leq 1$, one has $m \geq 0$). Then $\mathfrak{a} = p^m\mathbb{Z}_p$, because $y = p^n u' \in \mathfrak{a}$, $u' \in \mathbb{Z}_p^*$, implies $n \geq m$, hence $y = (p^{n-m}u')p^m \in p^m\mathbb{Z}_p$. The homomorphism

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}_p/p^n\mathbb{Z}_p \\ a & \longmapsto & a \mod p^n\mathbb{Z}_p \end{array}$$

has kernel $p^n\mathbb{Z}$ and is surjective. Indeed, for every $x \in \mathbb{Z}_p$, there exists by Proposition 4.15 an $a \in \mathbb{Z}$ such that

$$|x - a|_p \leq p^{-n}$$

i.e. $v_p(x-a) \geq n$, therefore $x - a \in p^n\mathbb{Z}_p$ and hence, $x \equiv a \mod p^n\mathbb{Z}_p$. So we obtain an isomorphism

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

□

Using this result, we obtain, for every $n \geq 1$, a surjective homomorphism

$$\varphi_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

It is clear that the family of these homomorphisms (φ_n) yields a homomorphism

$$\begin{array}{rccc} \varphi : & \mathbb{Z}_p & \longrightarrow & \varprojlim \mathbb{Z}/p^n\mathbb{Z} \\ & x & \longmapsto & (\varphi_1(x), \varphi_2(x), \dots) \end{array}$$

Proposition 4.17. *The homomorphism*

$$\begin{array}{rccc} \varphi : & \mathbb{Z}_p & \longrightarrow & \varprojlim \mathbb{Z}/p^n\mathbb{Z} \\ & x & \longmapsto & (\varphi_1(x), \varphi_2(x), \dots) \end{array}$$

is an isomorphism.

Proof. If $x \in \mathbb{Z}_p$ is mapped to zero, this means that $x \in p^n\mathbb{Z}_p$ for all $n \geq 1$, i.e. $|x|_p \leq p^{-n}$ for all $n \geq 1$, so that $|x|_p = 0$, and thus $x = 0$. This shows injectivity.

An element of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is given by a sequence of partial sums

$$s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu, \quad 0 \leq a_\nu < p$$

This sequences give us a Cauchy sequence in $\mathbb{Z}_p$ because, for $n > m$, one has

$$|s_n - s_m|_p = |\sum_{\nu=m}^{n-1} a_\nu p^\nu|_p \leq \max_{m \leq \nu < n} \{|a_\nu p^\nu|_p\} \leq p^{-m}$$

and thus, converges to an element

$$x = \sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p$$

Since

$$x - s_n = \sum_{\nu=n}^{\infty} a_\nu p^\nu \in p^n \mathbb{Z}_p$$

one has $x \equiv s_n \mod p^n$ for all n, i.e., x is mapped to the element of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ which is defined by the given sequence $(s_n)_{n\in\mathbb{N}}$. This shows surjectivity. □

Remark 4.18. The elements on the right hand side of the isomorphism

$$\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

are given formally by the sequences of partial sums s_n. On the left, however, these sequences converge with respect to the absolute value and yield elements of $\mathbb{Z}_p$ as convergent infinite series $x = \sum_{\nu=0}^{\infty} a_\nu p^\nu$.

4.3 Galois extensions of $\mathbb{Q}_p$. A brief summary

With a little bit more work we could now complete the algebraic closure of $\mathbb{Q}_p$, which is sometimes denoted as $\mathbb{C}_p$. One would have to study valuations and completions in order to achieve it. Information about this can be found on Chapter II, sections 3 and 4 of [8] and the completion of $\overline{Q_p}$ can be found in Chapter III of [7].[1]

The structure of Galois extensions of $\mathbb{Q}_p$ is discussed in detail in [10] and all of the assertions in this example are proved there in Chapter IV §1 and §2. Such extensions are constructed as a tower of three extension $\mathbb{Q}_p \subseteq E \subseteq L \subseteq K$ in the following manner:

1. The (unramified) extension $E \mid \mathbb{Q}_p$ has Galois group $\mathrm{Gal}(E \mid \mathbb{Q}_p) \cong \mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

2. The (tamely ramified) extension $L \mid E$ has Galois group $\mathrm{Gal}(L \mid E) \cong \mathbb{Z}/m\mathbb{Z}$ for m such that $(m, p) = 1$.

3. Finally, the (wildly ramified) extension $K \mid L$ has Galois group $\mathrm{Gal}(K \mid L) \cong P$, where P is a group of order p^k for some positive integer k.

4. The Galois group of the extension $K \mid E$ is a semi-direct product, that is, $\mathrm{Gal}(K \mid E) \cong P \rtimes \mathbb{Z}/m\mathbb{Z}$ subject to the constraints on m above.

[1] A summary of this topics can be found in `https://wstein.org/129/projects/hamburg/Project.pdf`

This characterization tells us that not every group can be realized as a Galois group over $\mathbb{Q}_p$. For example, A_5, the alternating group is not a Galois group over $\mathbb{Q}_p$.

The structure of the absolute Galois group of $\mathbb{Q}_p$ is fairly complicated. In particular, many non-abelian groups are quotients of $\mathrm{Gal}(\overline{\mathbb{Q}_p} \mid \mathbb{Q}_p)$, while A_5 is not.

Finally, we would like to remark that the characterization of $\mathbb{Q}_p$ lineal field automorphisms of $\mathbb{C}_p$ is still an unsolved problem.

Bibliography

[1] Emil Artin and Otto Schreier. Algebraische konstruktion reeller körper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):85–99, 1927.

[2] N. Bourbaki. *Éléments de mathématique. Topologie générale. Chapitres 1 à 4*. Hermann, Paris, 1971.

[3] Frederick Michael Butler. Infinite galois theory. `http://faculty.ycp.edu/~fbutler/MastersThesis.pdf`. Accessed: 2018-01-19.

[4] Mike Hamburg. Construction of $\mathbb{C}_p$ and extension of p-adic valuations to $\mathbb{C}$. `https://wstein.org/129/projects/hamburg/Project.pdf`. Accessed: 2018-01-19.

[5] Nathan Jacobson. *Basic algebra. I*. W. H. Freeman and Company, New York, second edition, 1985.

[6] Nathan Jacobson. *Basic algebra. II*. W. H. Freeman and Company, New York, second edition, 1989.

[7] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[8] Jürgen Neukirch. *Algebraic Number Theory*. Translated from German by Schappacher, N.

[9] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[10] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[11] Stephen S. Shatz. *Profinite groups, arithmetic, and geometry*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972. Annals of Mathematics Studies, No. 67.

[12] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1998.