DRP Project: Galois Theory and Profinite Groups

JIN QIAN

ABSTRACT. This paper provides a self-contained exposition of classical and modern Galois theory that culminates in the profinite-group viewpoint of infinite Galois extensions. We begin by reviewing field extensions, algebraic and transcendental elements, minimal polynomials, and the tower law, laying a linear-algebraic foundation for later results. After constructing splitting fields via Kronecker's theorem, we introduce automorphism groups of extensions and develop the concepts of separability, normality, and finite Galois extensions. The finite Fundamental Theorem of Galois Theory is presented together with explicit computations that illustrate its field–subgroup correspondence.To pass to the infinite setting, we equip automorphism groups with the Krull topology and assemble them as inverse limits of finite Galois groups, obtaining compact, totally disconnected, Hausdorff (profinite) groups. A concise survey of the requisite topology—product spaces, compactness, Hausdorffness, and inverse limits—precedes the formulation of the infinite Fundamental Theorem. We prove that intermediate fields of an arbitrary Galois extension L/K correspond bijectively to closed subgroups of the profinite group $\mathrm{Gal}(L/K)$, with finite subextensions matching open subgroups.

CONTENTS

Date: May,2025.

1. Field Extensions

Definition 1.1 A set F with addition and multiplication is a field if the following conditions hold.

(1) F is an abelian group under addition.

(2) $F\backslash\{0\}$ is an abelian group under multiplication.

(3) The distributive law holds: $a(b+c) = ab + ac$.

Definition 1.2 If a field K is a subfield of a field L, then $K \subseteq L$ is a field extension.
Example: $Q \subseteq Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\}$ is a field extension of Q. In this paper, we will explore some uncommon fields and study their properties.

Proposition 1.3 A field extension $K \subseteq L$ is a vector space with scalars from K.

2. Algebraic Extensions

Definition 2.1 Let $K \subseteq L$ be a field extension. We say that an element $\alpha \in L$ is *algebraic* over K if there exists a nonzero polynomial $f \in K[X]$ such that $f(\alpha) = 0$. If such a polynomial does not exist, α is *transcendental* over K.

If $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, then we say that α is an algebraic number.

Definition 2.2 If $\alpha \in L$ is algebraic over K, then any non-zero polynomial of the least possible degree among all the polynomials $f \in K[X]$ such that $f(\alpha) = 0$ is called a minimal polynomial of α over K. The degree of f is called the degree of α over K. *The minimal polynomial*, is the unique minimal polynomial whose highest coefficient equals 1.

Theorem 2.3 Simple Extension Theorem

(1) If $a \in L$ is *algebraic* over K, then each element in $K(\alpha)$ can be uniquely written as $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$ where $a_i \in K$ and n is the degree of the minimum polynomial of α over K. Thus $[K(\alpha) : K] = n$ and $1, \alpha, ..., \alpha^{n-1}$ is a basis of $K(\alpha)$ over K.

(2) If $a \in L$ is *transcendental* over K, then $K[\alpha] \cong K[X]$, $K[X]$ is the ring of polynomial over K.

Proof. Let p be a minimal polynomial of α over K and consider the following ring homomorphism.

$$\phi : K[X] \to K[\alpha]$$

where $\phi(f(X)) = f(\alpha)$.

$$Ker(\phi) = \{f \in K[X] : \phi(f) = \phi(\alpha) = 0\} = (p(X))$$

Every polynomial that has α as a root is a multiple $p(X)$. Trivially, the image of ϕ is the entire ring $K[\alpha]$. By ring homomorphism theorem, we have $K[X]/Ker(\phi) \cong K[X]/(p(X)) \cong K[\alpha]$. Since every class in $K[X]/(p(X))$ can be written uniquely as

$$a_0 + a_1X + a_2X^2 + ...a_nX^{n-1}, a_i \in K$$

Hence, by the ring homomorphism, every element in $K[\alpha]$ can be written uniquely in the form

$$a_0 + a_1\alpha + a_2\alpha + ... + a_n\alpha^{n-1}, a_i \in K$$

Since p is a minimal polynomial over K, it's irreducible. $K[X]/(p(X)) \cong K[\alpha]$ is a field if and only if p is irreducible. $K[\alpha]$ is a field and clearly has basis $\alpha, ..., \alpha^{n-1}$. Part (2) of the theorem is trivial. ■

Example: What is the smallest field extension of $\mathbb{Q}$ that contains $\alpha = \sqrt[3]{2}$? Find its basis and dimension. Clearly, α is algebraic over $\mathbb{Q}$ since $f(X) = X^3 - 2 \in \mathbb{Q}[X]$ and $f(\alpha) = 0$. Applying the *Simple Extension Theorem*, $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$ is a basis of $\mathbb{Q}(\sqrt[3]{2})$.

Definition 2.4 Let $K \subseteq L$ and X be a subset of L, then $K(X)$ denotes the intersection of all subfields of L is the least subfield of L that contains both K and X. If $X = \{\alpha_1, ..., \alpha_n\}$, we write $K(X) = K(\alpha_1, ..., \alpha_n)$. If $X = K'$ is a subfield of L, we denote $K(K')$ as KK' and call it the *compositum* of K and K'

Definition 2.5 An extension $K \subseteq L$ is *algebraic* if all elements in L are algebraic over K. It is *finite* if $[L : K] \neq \infty$. We say that the extension $K \subseteq L$ is finitely generated if $L = K(\alpha_1, ..., \alpha_n), \alpha_i \in L$.

Now, let's think about a finite field extension, say $L = K(\alpha_1, ..., \alpha_n), \alpha_i \in L$. How do we find its basis and dimension? For example, what is the basis and dimension for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We can slowly work this out, but introducing the *Tower Law* will be more convenient.

Theorem 2.6 Tower Law

Let $K \subseteq L$ and $L \subseteq M$ be finite field extensions. Then $K \subseteq M$ is a field extension and

$$[M : K] = [M : L][L : K]$$

Proof. Let $e_i, i = 1, ..., l$ be basis of L over K; let $f_j, j = 1, ..., m$ be basis of M over L. Let $x \in M$, then there is a unique presentation $x = \sum_{j=1}^{m} l_j f_j,\ \ l_j \in L$. For each l_j there is a unique presentation $l_j = \sum_{i=1}^{l} a_{ij} e_i\ ,\ a_{ij} \in K$. Now, we write

$$x = \sum_{j=1}^{m} l_j f_j = \sum_{j=1}^{m} \sum_{i=1}^{l} a_{ij} e_i f_j$$

This shows x is a unique linear combination of $e_i f_j$ and lm products $e_i f_j$ form a basis of M over K. ■

Example: Let's revisit the finite field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We express this extension as the following

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$$

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Theorem 2.7 A field extension $K \subseteq L$ is finite if and only if it is algebraic and finitely generated.

Proof.

($\Rightarrow$) Suppose a field extension $K \subseteq L$ is finite. Then there must be a basis $\beta_1, ..., \beta_n$ of L over K, so that $L = K(\beta_1, ..., \beta_n)$, i.e. L is finitely generated over K. To prove it's algebraic, let $x \in L$ and consider the powers $\{1, x, x^2, ..., x^n\}$. There are $n + 1$ such elements, so they must be linearly dependent, i.e.

$$a_o + a_1 x + a_2 x^2 + ... + a_n x^n = 0, a_i \in K$$

not $a_i = 0$. Hence x is an algebraic element over K, i.e.L is an algebraic extension over K.

($\Leftarrow$) Suppose $K \subseteq L$ is algebraic and finitely generated, i.e. $L = K(\alpha_1, ..., \alpha_k)$. We have the following

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq ... \subseteq K(\alpha_1, \alpha_2, ..., \alpha_k)$$

For every $i = 0, ..., n - 1$ we have α_{i+1} algebraic over K, so it's algebraic over $K(\alpha_1, ..., \alpha_i)$. Therefore, the extension $K(\alpha_1, ..., \alpha_i) \subseteq K(\alpha_1, ..., \alpha_i, \alpha_{i+1})$ is finite. Hence the extension $K \subseteq L$ is finite as its degree is the product of degrees $[K(\alpha_1, ..., \alpha_i) : K(\alpha_1, ..., \alpha_i, \alpha_{i+1})]$. ■

Remark: If a field extension $K \subseteq L$ is finitely generated, it's not sufficient to show the field extension is finite. The extension being algebraic is a necessary condition. Let's consider an interesting example where $\mathbb{Q}(\pi)$ is finitely generated, but not algebraic over $\mathbb{Q}$.This field extension is not finite, $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$.

Theorem 2.8 Let $K \subseteq L$. All elements in L algebraic over K form a field

Proof. Let $\alpha, \beta \in L$ be two algebraic elements over K. Then the extensions $K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$ are finite. Hence, the extensions are algebraic. $\alpha + \beta \in K(\alpha, \beta)$, $\alpha\beta \in K(\alpha, \beta)$, $\alpha/\beta \in L$. The set of algebraic elements in L is closed under the operations. Hence all elements in L algebraic over K form a field. ■

3. Splitting Fields

Definition 3.1 K is a field and $f \in K[x]$, we say L is a *splitting field* of f over K if $L = K(\alpha_1, ..., \alpha_n)$ and $f(X) = a(X - \alpha_1)...(X - \alpha_n),\ a \in K$. Sometimes, we denote the splitting field of f over K as K_f.

Definition 3.2 $\tau : K \to K'$ is an *embedding* of the field K if τ is an injective function such that $\tau(x + y) = \tau(x) + \tau(y)$ and $\tau(xy) = \tau(x)\tau(y),\ x, y \in K$.

τ can be extended to the *embedding* of the polynomial rings $\tau : K[X] \to K'[X]$

$$\tau(f(X)) = \tau(a_n)X^n + ... + \tau(a_1)X + \tau(a_0)$$

$$f(X) = a_nX^n + ... + a_1X + a_0 \in K[X]$$

If $\tau(K) = K'$, then the function is an *isomorphism* of the field K and K'.

Theorem 3.3 Kronecker's Theorem

(1) If f is an *irreducible* polynomial over K, then there exists a field $K \subseteq L$ such that $L = K(\alpha)$ and $f(\alpha) = 0$.

(2) If $\tau : K \to K'$ is a field isomorphism, f an *irreducible* polynomial over K, $L = K(\alpha)$, where $f(\alpha) = 0$ and $L' = K'(\alpha')$, where $\tau(f)(\alpha') = 0$, then there is an isomorphism $\sigma : K(\alpha) \to K'(\alpha')$.

$$\begin{tikzcd} K(\alpha) \arrow[r, "\sigma"] & K'(\alpha') \\ K \arrow[u] \arrow[r, "\tau"] & K' \arrow[u] \end{tikzcd}$$

$\sigma(\alpha) = \alpha'$ and $\sigma|_K = \tau$.

Proof.

(1) Let $L = K[X]/(f(X))$, since f is irreducible in $K[X]$, L is a field. The class $[X] = \alpha$ is a solution in L of the equation $f(X) = 0$ and $L = K(\alpha)$.

(2) Consider the isomorphism $\tau : K \to K'$. Extend τ to the embedding of the polynomial rings $\tau : K[X] \to K'[X]$. This maps the irreducible polynomial $f(X)$ onto the irreducible polynomial $\tau(f)(X)$ in $K'[X]$. Now, we have an isomorphism of the quotient rings:

$$\tau' : K[X]/(f(X)) \to K'[X]/(\tau(f)(X))$$

such that the class of $[X] = \alpha$ is mapped onto $[X] = \alpha'$ in the second ring. Since $K[X]/(f(X)) = K(\alpha)$ and $K'[X]/(\tau(f)(X)) = K'[\alpha']$, we have $\tau' = \sigma$ as the required extension of τ. ■

Corollary 3.4

(1) Every polynomial $f \in K[X]$ has a splitting field over K.

(2) If $\tau : K \to K'$ is a field isomorphism, L is a splitting field of a polynomial $f \in K[X]$ and L' is the splitting field of $\tau(f) \in K'[X]$, there exists an isomorphism $\sigma : L \to L'$.

$$\begin{tikzcd}
L \arrow[r, "\sigma"] & L' \\
K \arrow[u] \arrow[r, "\tau"] & K' \arrow[u]
\end{tikzcd}$$

Remark: To prove this corollary, we just apply inductive argument.

4. Automorphisms and Galois Groups

Definition 4.1 Let L be a field. An automorphism of L is a bijection $\sigma : L \to L$ such that $\forall x, y \in L$

(1) $\sigma(x + y) = \sigma(x) + \sigma(y)$

(2) $\sigma(xy) = \sigma(x)\sigma(y)$

If $K \subseteq L$ is a field extension, an automorphism $\sigma : L \to L$ is called a *K-automorphism*, if $\forall x \in K$, $\sigma(x) = x$.

Proposition 4.2 All K-automorphisms of L form a group under the composition of automorphisms.The group is called *Galois group* of L over K, denoted as $Gal(L/K)$.

Definition 4.3 Let G be a group of automorphisms of L, we define $L^G = \{x \in L : \forall\sigma \in G, \sigma(x) = x\}$.

Remark: It's trivial to see that L^G is a subfield of L. To construct elements of L^G, we introduce the *trace* (Tr_G) and the *norm* (Nr_G) with respect to G.

$$Tr_G(\alpha) = \sum_{\sigma \in G} \sigma(\alpha), \quad Nr_G = \prod_{\sigma \in G} \sigma(\alpha), \quad \alpha \in L$$

Tr_G and $Nr_G \in L^G$, and for all $\alpha, \beta \in L$, we have $Tr_G(\alpha + \beta) = Tr_G(\alpha) + Tr_G(\beta)$ and $Nr_G(\alpha\beta) = Nr_G(\alpha)Nr_G(\beta)$. It easily follows from the definitions of trace, norm, and automorphisms.

Theorem 4.4 Dedekind's Lemma

Let $\sigma_1, \sigma_2, ..., \sigma_n$ be distinct automorphisms of a field L, if the equality: $a_1\sigma_1(x) + a_2\sigma_2(x) + ... + a_n\sigma_n(x) = 0$, where $a_i \in L$, holds for all $x \in L$, then $a_1 = a_2 = ... = a_n = 0$.

Proof.

We will use induction to prove this theorem. Base case: $n = 1$, then $a_1\sigma_1(x) = 0$ for all $x \in L$. This forces $a_1 = 0$, so the base case holds. Now, assume that the theorem holds when the number of isomorphisms is less than n, where $n > 1$. We have:

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_n\sigma_n(x) = 0 \tag{1}$$

This equality (1) holds for all $x \in L$, so we can choose an arbitrary $\alpha \in L$ and replace x by αx:

$$a_1\sigma_1(\alpha)\sigma_1(x) + a_2\sigma_2(\alpha)\sigma_2(x) + \cdots + a_n\sigma_n(\alpha)\sigma_n(x) = 0 \tag{2}$$

Multiply the equality (1) by $\sigma_n(\alpha)$ and subtract it from the equality (2):

$$a_1(\sigma_n(\alpha) - \sigma_1(\alpha))\sigma_1(x) + a_2(\sigma_n(\alpha) - \sigma_2(\alpha))\sigma_2(x) + ... + a_{n-1}(\sigma_n(\alpha) - \sigma_{n-1}(\alpha))\sigma_{n-1}(x) = 0 \tag{3}$$

By our inductive assumption, all the coefficients in equality (3) must be zero, i.e. $a_i(\sigma_n(\alpha) - \sigma_i(\alpha)) = 0$ for $i = 1, ..., n-1$. Now, since all automorphisms are distinct, this forces $a_i = 0$ for $i = 1, ..., n-1$. Let's revisit equality (1), we have $a_n\sigma_n(x) = 0$ for all $x \in L$, which again forces $a_n = 0$. ■

Proposition 4.5

If G is a group of automorphisms of L (finite or infinite), then L^G is a subfield of L and $[L : L^G] = |G|$.

Proposition 4.6 Let $f(X) \in K[X]$ and let L/K be a field extension of K. If $\sigma : L \to L$ is a K-automorphism and if $\alpha \in L$ is a root of $f(X)$, then $\sigma(\alpha)$ is also a root of $f(X)$.

Theorem 4.7 If $f(X) \in K[X]$ has n distinct roots in its splitting field L, then $Gal(L/K)$ is isomorphic to a subgroup of the symmetric group S_n, and its order divides $n!$.

Proof.

Let $T := \{\alpha_1, \alpha_2, ..., \alpha_n\}$ be the set of roots of $f(X)$ in L. By Proposition 4.3, if $\sigma \in Gal(L/K)$, $\sigma(T) = T$. The map $Gal(L/K) \to S_T$, defined by $\sigma \mapsto \sigma|_T$ is clearly a bijective homomorphism, and $S_T \cong S_n$. ■

5. Normal, Separable, and Galois Extensions

Definition 5.1 A field extension $K \subseteq L$ is called *normal*, if every irreducible polynomial $f(X) \in K[X]$, which has one zero in L, has all its zeros in L, i.e. L contains a splitting field of $f(X)$.

Proposition 5.2 A field extension $K \subseteq L$ is normal if and only if L is a splitting field of polynomials with coefficients in K.

Definition 5.3

(1) An irreducible polynomial $f(X) \in K[X]$ is *separable* over K, if it has no multiple zeros.

(2) $\alpha \in L \supseteq K$ is a *separable element* over K, if it is algebraic and its minimal polynomial over K is separable.

(3) The extension L/K itself is called *separable* if every element of L is separable over K. For finite extensions this is equivalent to saying that L/K admits the maximum possible number $[L : K]$ of K-embeddings into an algebraic closure.

Definition 5.4 Let $K \subseteq L$ be a finite field extension. We say that L/K is *Galois* if it is simultaneously *normal* and *separable*.

Proposition 5.5 For a finite extension L/K the following statements are equivalent:

(1) L/K is Galois.

(2) L is the splitting field over K of a *separable* polynomial.

(3) $|(L/K)| = [L : K]$.

(4) The fixed field of (L/K) equals K, i.e. $L^{(L/K)} = K$.

6. Finite Galois Theory

Let $K \subseteq L$ be a field extension and write

$$\mathcal{F} \;=\; \{\, M \mid K \subseteq M \subseteq L \,\}, \quad \mathcal{G} \;=\; \{\, H \leqslant (L/K) \,\}.$$

Define two order-reversing maps

$$f : \mathcal{G} \longrightarrow \mathcal{F}, \qquad f(H) \;=\; L^H \;:=\; \{\, x \in L \mid \sigma(x) = x \text{ for every } \sigma \in H \,\},$$

$$g : \mathcal{F} \longrightarrow \mathcal{G}, \qquad g(M) \;=\; (L/M) \;=\; \{\, \sigma \in (L/K) \mid \sigma|_M = \mathrm{id}_M \,\}.$$

Theorem 6.1 Fundamental Theorem of Galois Theory
Let L/K be a finite Galois extension with group $G = (L/K)$.

(1) The maps f and g are inverse bijections $\mathcal{G} \overset{f}{\underset{g}{\rightleftarrows}} \mathcal{F}$ that reverse inclusion.

(2) A subgroup $H \leqslant G$ is normal in G iff the field L^H is Galois over K; in that case $(L^H/K) \cong G/H$.

(3) For every subgroup $H \leqslant G$ one has $[L^H : K] = |G : H|$.

Proof. We must prove that $f \circ g = \mathrm{id}_{\mathcal{F}}$ and $g \circ f = \mathrm{id}_{\mathcal{G}}$.

(i) Evaluate $f \circ g$. Choose any intermediate field M with $K \subseteq M \subseteq L$. By definition,

$$g(M) = G(L/M) \quad \text{and} \quad f\big(g(M)\big) = L^{G(L/M)}.$$

Since $L \supseteq M$ is itself a finite Galois extension (Prop.5.5) tells us that the fixed field of the full automorphism group $G(L/M)$ is exactly M: $L^{G(L/M)} = M$. Hence $f \circ g$ acts as the identity on $\mathcal{F}$.

(ii) Evaluate $g \circ f$. Noow take a subgroup $H \leqslant G = (L/K)$. Because $f(H) = L^H$, we have

$$g\big(f(H)\big) = \big(L/L^H\big).$$

The group of automorphisms of L that fix L^H point-wise is precisely H itself, so $g \circ f$ is the identity on $\mathcal{G}$.

(iii) Order reversal. If $H_1 \subseteq H_2$ then $L^{H_2} \subseteq L^{H_1}$, so f reverses inclusion; the same reasoning applied to g gives the dual statement for intermediate fields.

Consequently, f and g are mutually inverse bijections that invert the partial orderings. ■

7. Topology Background for Infinite Galois Theory

Definition 7.1 (Topological space)**.** A *topological space* is a pair $(X, \mathscr{T})$ where $\mathscr{T} \subseteq 2^X$ (the "open" sets) satisfies (i) $\varnothing, X \in \mathscr{T}$; (ii) arbitrary unions of opens are open; (iii) finite intersections of opens are open. A set is *closed* if its complement is open.

Definition 7.2 (Continuous map, basis, discrete space)**.** (1) A function $f\colon X \to Y$ between spaces is *continuous* if $f^{-1}(U)$ is open in X whenever U is open in Y.

(2) A collection $\mathcal{B} \subseteq \mathscr{T}$ is a *basis* if every open set is a union of elements of $\mathcal{B}$.

(3) The *discrete topology* on a set X is the topology $\mathscr{T} = 2^X$; a space with the discrete topology is called *discrete*.

Definition 7.3 (Hausdorff, compact)**.** A topological space X is *Hausdorff* if any two distinct points admit disjoint open neighbourhoods, and *compact* if every open cover has a finite subcover.

Definition 7.4 (Product topology)**.** For a family of spaces $\{X_i\}_{i\in I}$ the *product topology* on $\prod_{i\in I} X_i$ is generated by sets $\prod_i U_i$ with $U_i \subseteq X_i$ open and $U_i = X_i$ for all but finitely many indices i.

Proposition 7.5. Every finite discrete space is compact and Hausdorff.

Proof. Any open cover of a finite set contains finitely many opens, hence compact; distinct singletons are closed, so their complements form disjoint opens, giving the Hausdorff property. □

Definition 7.6 (Directed set)**.** A non-empty partially ordered set $(I, \leqslant)$ is *directed* if for any $i, j \in I$ there exists $k \in I$ with $i \leqslant k$ and $j \leqslant k$.

Definition 7.7 (Inverse system and inverse limit)**.** Given a directed set I, an *inverse system* $\big(X_i, \pi_{ij}\big)$ consists of spaces X_i and continuous maps $\pi_{ij}\colon X_j \to X_i$ for $i \leqslant j$ such that $\pi_{ii} = \mathrm{id}$ and $\pi_{ik} = \pi_{ij} \circ \pi_{jk}$. Its *inverse limit* is the subspace

$$\varprojlim_{i\in I} X_i = \Big\{(x_i) \in \prod X_i : \pi_{ij}(x_j) = x_i\Big\},$$

with the subspace topology from the product.

Definition 7.8 (Totally disconnected, profinite space/group)**.** A space is *totally disconnected* if its only connected subsets are singletons. A *profinite space* is compact, Hausdorff, and totally disconnected. A *profinite group* is a topological group whose underlying space is profinite.

Definition 7.9 (Topological group)**.** A *topological group* is a group G equipped with a topology for which multiplication $(x, y) \mapsto xy$ and inversion $x \mapsto x^{-1}$ are continuous.

Proposition 7.10. If each X_i in Definition7.7 is compact Hausdorff then $\varprojlim X_i$ is compact Hausdorff. Consequently, any inverse limit of finite discrete groups is a profinite group.

Proof. By Tychonoff, the product $\prod X_i$ is compact Hausdorff. The limit set is closed (hence compact) and inherits Hausdorffness. Finite discrete groups satisfy Proposition7.5. □

Definition 7.11 (Krull topology)**.** For a Galois extension L/K (finite or infinite) set

$$G = (L/K) = \varprojlim_{E/K \text{ finite Galois}} (E/K).$$

Equip G with the inverse-limit topology; a sub-basis of open neighbourhoods of 1 is given by the kernels of the natural restriction maps $G \to (E/K)$.

Proposition 7.12. With the Krull topology, $G = (L/K)$ is a profinite group.

Proof. Each finite layer (E/K) is a finite discrete group, hence compact Hausdorff (Proposition7.5). Apply Proposition7.10. □

Proposition 7.13 (Field–subgroup dictionary)**.** For $G = (L/K)$ as in Definition7.11:

Closed subgroup $H \leqslant G$	Intermediate field L^H
Open subgroup H	L^H/K finite
$\lvert G : H\rvert < \infty$	$\deg(L^H/K) = \lvert G : H\rvert$

Proof. Closedness follows because the fixed-point set of a continuous group action is closed; kernels of the restriction maps are open and of finite index, yielding the second row. The degree–index equality is the finite Fundamental Theorem applied to each layer of the inverse system. □

$$\begin{tikzcd}
& (L/E_1) \arrow[dr, dash] & (L/E_2) \arrow[l] \arrow[d, dash] & (L/E_3) \arrow[l] \arrow[dl, dash] & \cdots \arrow[l] \\
& & {} & & \\
G = \varprojlim(L/E_i) \arrow[uur, "\pi_1"] \arrow[uurr, bend left, "\pi_2"] \arrow[uurrr, bend left, "\pi_3"] \arrow[urr, dashed, dash] & & & &
\end{tikzcd}$$

Armed with these topological notions, one extends the finite Fundamental Theorem of Galois Theory to arbitrary Galois extensions by interpreting "subgroup" as "*closed subgroup*" and "finite" as "*open*" inside the profinite group (L/K).

8. Infinite Galois Theory

Throughout, K is a field and L/K an algebraic extension. All topological notions are those from Chapter 7, and every automorphism group carries the Krull topology of Definition7.11.

Definition 8.1 (Separable, normal, Galois).

(1) L/K is *separable* if every $\alpha \in L$ is the root of a separable polynomial over K.

(2) L/K is *normal* if every irreducible $f \in K[x]$ that has a root in L splits completely in L.

(3) A *Galois extension* is algebraic, separable, and normal.

Definition 8.2 (Absolute Galois group). Fix a separable closure $\overline{K}$ of K and set

$$G_K \;=\; (\overline{K}/K) \;=\; \{\sigma \in (\overline{K}) \mid \sigma|_K = \mathrm{id}_K\}.$$

With the Krull topology, G_K is profinite (Proposition7.12).

Theorem 8.3 (Fundamental theorem of infinite Galois theory). Let L/K be (possibly infinite) Galois and write $G = (L/K)$ with the Krull topology. There is an inclusion-reversing bijection

$$K \subseteq E \subseteq L \;\longleftrightarrow\; \text{closed subgroups } H \leqslant G, \qquad E \mapsto (L/E), \quad H \mapsto L^H,$$

satisfying:

(1) E/K is finite iff (L/E) is *open* in G.

(2) E/K is normal iff (L/E) is *normal* in G.

(3) For each closed $H \leqslant G$ the natural map $G/H \to (L^H/K)$ is a topological isomorphism.

Proof. View G as the inverse limit of its finite Galois quotients. The classical (finite) correspondence holds on each layer; passing to the limit gives the result. Details appear in *Artin–Tate,Chap. VI.* □

Proposition 8.4 (Fixed-field diagram). For a closed subgroup $H \leqslant G = (L/K)$ the diagram

$$\begin{tikzcd}
G \arrow[r, bend left, hook] \arrow[d, two heads] & (L^H/K) \\
G/H \arrow[ur, "\sim"'] &
\end{tikzcd}$$

commutes and the diagonal arrow is an isomorphism.

Proof. Restriction kills H, hence factors through G/H; bijectivity follows from Theorem8.3(3). □

Example 8.5 (Finite fields). For $\mathbb{F}_q$ ($q = p^m$) the Frobenius $\varphi : x \mapsto x^q$ generates $(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$. Finite extensions $\mathbb{F}_{q^n}$ correspond to open subgroups $\langle \varphi^n \rangle$.

Corollary 8.6 (Inverse-limit descriptions). Let $\mathcal{E}$ be the directed set of finite Galois subextensions E/K inside L. Then

$$L \cong \varinjlim_{E \in \mathcal{E}} E, \qquad (L/K) \cong \varprojlim_{E \in \mathcal{E}} (E/K),$$

the latter with its profinite topology.

Proof. L equals the union of its finite Galois subfields; Proposition7.10 identifies the inverse limit of groups. □

Proposition 8.7 (Tower law). For Galois extensions $L/F/K$ there is an exact sequence

$$1 \longrightarrow (L/F) \longrightarrow (L/K) \longrightarrow (F/K) \longrightarrow 1.$$

Proof. Restriction onto F is surjective; its kernel is (L/F). □

Theorem 8.8 (Hilbert 90, cohomological form). If L/K is Galois with group G, then $H^1(G, L^\times) = 1$. Equivalently, for $a, b \in L^\times$, $\sigma(a)/a = \sigma(b)/b$ for all $\sigma \in G$ implies $a/b \in K^\times$.

Proof. See *Lang, Algebraic Number Theory*, Chap. VIII. □

Dual diagrams (fields ↔ groups)

$$\begin{tikzcd}
& L \arrow[dl, dash, "(L/E_1)"'] \arrow[dr, dash, "(L/E_2)"] & \\
E_1 \arrow[dr, dash] & & E_2 \arrow[dl, dash] \\
& K &
\end{tikzcd}
\qquad
\begin{tikzcd}
& G \arrow[dl, dash] \arrow[dr, dash] & \\
H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\
& \{1\} &
\end{tikzcd}$$

Left: lattice of intermediate fields. Right: lattice of closed subgroups. Arrows are inclusions, illustrating the bijection of Theorem8.3.

References

[1] J. Brzeziński, *Galois Theory Through Exercises*, Springer Undergraduate Mathematics Series, Springer, 2018.

[2] J. S. Wilson, *Profinite Groups*, London Mathematical Society Monographs, Clarendon Press (OUP), 1998.

[3] I. Stewart, *Galois Theory*, 4th ed., Chapman & Hall/CRC, Boca Raton, 2015.

[4] D. J. H. Garling, *A Course in Galois Theory*, Cambridge University Press, Cambridge, 1986.