

A personal note on infinite dimensional Galois theory

by Jinhyun Park
January 30, 2004

1. INTRODUCTION

Let K be a separable normal extension, i.e. Galois extension of a field k with $G = \text{Gal}(K/k)$. Classical Galois theory tells us that when $[K, k] < \infty$, there is a one to one correspondence between intermediate fields $K \supset L \supset k$ and subgroups $H \subset G$ by

$$\mathcal{F} = \{L | K \supset L \supset k\} \longrightarrow \mathcal{G} = \{H | H < G\}$$

$$L \xrightarrow{\phi} \text{Gal}(K/L)$$

$$K^H \xleftarrow{\psi} H,$$

and L/k is a Galois extension if and only if $\text{Gal}(K/L) \triangleleft \text{Gal}(K/k)$. The proof of it depends on counting which makes use of the finiteness of $[K, k]$. For infinite dimensional case, hence we need to modify it a little bit.

2. INFINITE DIMENSIONAL CASE

For infinite dimensional case, the problem we have is that, unlike the finite dimensional case, \mathcal{G} is too big, compared with \mathcal{F} . But, one direction of the classical theory still can be done as follows:

Lemma 2.1. *Let $K \supset L \supset k$ be fields and K/k be Galois. Then, with above notations, $\psi \circ \phi = \text{id}_{\mathcal{F}}$, i.e.*

$$\mathcal{F} \xrightarrow{\phi} \mathcal{G} \xrightarrow{\psi} \mathcal{F}$$

$$L \mapsto \text{Gal}(K/L) \mapsto K^{\text{Gal}(K/L)} = L.$$

Proof. Note that $K^{\text{Gal}(K/L)} \supset L$ is obvious, so that we prove that \subset is true. To do so, we show that any element ξ in $K - L$ is not fixed by $\text{Gal}(K/L)$.

Let L_1 be the splitting field of the minimal polynomial of ξ over L so that $K \supset L_1 \supset L$. Then, $1 < [L_1, L] < \infty$ and L_1/L is Galois, so that finite dimensional Galois theory tells us that there is $\sigma \in \text{Gal}(L_1/L)$ with $\sigma(\xi) \neq \xi$. By applying Zorn's lemma, σ then can be extended to an element $\sigma \in \text{Gal}(K/L)$ so that $\sigma(\xi) \neq \xi$. which means, $\text{Gal}(K/L)$ doesn't fix ξ . □

\mathcal{G} , however, is too big, so that to find a suitable subset of \mathcal{G} , we give the following topology on G .

Consider the collection of all K_i , $K \supset K_i \supset k$ with $[K_i : k] < \infty$ and K_i/k is normal, and let

$$G \triangleright G_i = \text{Gal}(K/K_i), \quad S_i = G/G_i = \text{Gal}(K_i/k).$$

If $K_i \supset K_j$, then there is a natural homomorphism

$$\phi_{ij} : S_i = \text{Gal}(K_i/k) \rightarrow S_j = \text{Gal}(K_j/k)$$

coming from restrictions so that S_i forms an inverse system of groups.

Claim. $G = \varprojlim S_i = \varprojlim G/G_i$, with $\phi_i : G \rightarrow G/G_i = S_i$, the canonical projection.

Proof. Note that $\varinjlim K_i = K$, (K/k being algebraic) so that any $\xi \in K$ lies in some K_i , and for all $\sigma \in G$, $\sigma(\xi) = (\phi_i \sigma)(\xi)$. Hence σ is uniquely determined by the knowledge of all the $\phi_i \sigma$. □

Each S_i is a finite group. Give it the discrete topology. And give G , the topology induced on it as the inverse limit, i.e. the crudest topology such that each ϕ_i is continuous, i.e. the base of open sets are given by the cosets of G_i , and in this case, any such open sets are also closed, because it is the complement of the union of all other open cosets. (See Atiyah-Macdonald, or J-P Serre's Cohomologie Galoisienne.)

Proposition 2.2. *With above topology, G is Hausdorff, compact and totally disconnected.*

Proof. In fact, these properties are general properties of profinite groups. Note that $\cap G_i = \{1\} = \{\sigma \in G \mid \sigma(\xi) = \xi\} = \{1\}$ so that it is Hausdorff. $G \subset \prod G/G_i$ is closed and each G/G_i is compact Hausdorff, hence G is compact. etc. □

Now the other direction of the Galois theory can be stated as follows:

Lemma 2.3. *Let $H < G$. Then, $H = \text{Gal}(K/L)$ for some field L , $K \supset L \supset k$ if and only if H is closed in G .*

Proof. (\Rightarrow) Let $H = \text{Gal}(K/L)$, let $\sigma \in \bar{H}$ in G , and let $\xi \in L$. If $\sigma\xi = \xi$, then, $\sigma \in H$ so that $\bar{H} = H$ implies that H is closed, hence done.

Let $K_0 \subset K$ be the splitting field of the minimal polynomial of ξ over k , so that K_0/k is Galois and $[K_0, k] \infty$. Let $G_0 = \text{Gal}(K/K_0)$, $S_0 = \text{Gal}(K_0/k)$, and $\phi : G \rightarrow S_0 = G/G_0$ be the projection. Since S_0 is discrete, $\phi_0 H \subset S_0$ is closed, and leave ξ fixed. Hence $\phi_0^{-1} \phi_0 H$ is closed in G and leave ξ fixed. Since σ lies in the closure of H , and $\phi_0^{-1} \phi_0 H$ is a closed set containing H , $\sigma \in \phi_0^{-1} \phi_0 H$ so that $\sigma(\xi) = \xi$.

(\Leftarrow) Let $H < G$ be closed and let $L = K^H$. Then, $H \subset \text{Gal}(K/L)$ is obvious. To show the other direction, let $\sigma \notin H$. Then, it is enough to show that $\sigma \notin \text{Gal}(K/L)$, i.e. there is an element of L not fixed by σ . H being closed, there is a basis element $N \ni \sigma$ not meeting H , i.e. there is a finite Galois extension K_1/k with $\phi_1 : G \rightarrow S_1 = \text{Gal}(K_1/k)$ such that $\phi_1 H \not\supset \phi_1 \sigma$. Let $K_2 = K_1^{\phi_1 H}$. K_2 is then fixed by H so that $K_2 \subset L$ and by construction, K_2 is not fixed by $\phi_1 \sigma$ by finite Galois theory of K_1/k . This implies that $\sigma \notin \text{Gal}(K/L)$. □

Hence by combining above two lemmas, we have the following theorem.

Theorem 2.4 (The fundamental theorem of Galois theory). *Let $K \supset k$ be an arbitrary Galois extension. Then, there is a one to one correspondence between fields L with $K \supset L \supset k$ and closed subgroups $H < G$.*

Example 2.5. Let $k = \mathbb{F}_q$ be a finite field, and let $K = \bar{k}$, its algebraic closure. We can describe $\text{Gal}(K/k)$.

For any n , there is a unique finite extension $K^{(n)}$ of k , which is Galois. Let $S^{(n)} = \text{Gal}(K^{(n)}/k)$. It is cyclic of order n and generated by the Frobenius map $\sigma : x \mapsto x^q$ i.e. $S^{(n)} \simeq \mathbb{Z}/(n)$ via $\sigma^\nu \mapsto \nu \pmod n$. We know that $K^{(m)} \supset K^{(n)}$ if and only if $n \mid m$ and $\phi_{m,n} : \mathbb{Z}/(m) \rightarrow \mathbb{Z}/(n)$ is just $\nu \pmod m \mapsto \nu \pmod n$. When $(m, n) = 1$, then $K^{(m)} K^{(n)} = K^{(mn)}$ and $S^{(mn)} \simeq S^{(m)} \times S^{(n)}$. Hence

$$G \simeq \prod_{p: \text{ prime}} \varprojlim S^{(p^\nu)} = \prod_{p: \text{ prime}} \varprojlim \mathbb{Z}/(p^\nu) = \prod_{p: \text{ prime}} \mathbb{Z}_p.$$