INFINITE GALOIS THEORY

BRIAN OSSERMAN

The fundamental theorem of Galois theory extends in a natural way to infinite Galois extensions, taking into account the natural profinite topology on the Galois group.

1. Basic properties

We can describe the Galois group of even an infinite Galois extension as an inverse limit of finite Galois groups.

Proposition 1.1. *If K/F is Galois, then the natural map*

$$\operatorname{Gal}(K/F) \to \varprojlim_{L/F \text{ finite Galois, } L\subseteq K} \operatorname{Gal}(L/F)$$

is an isomorphism.

Proof. The point is simply that K is the union of finite Galois subextensions L/F: indeed, this follows by considering the Galois closure of each element of K over F.

This means that every automorphism of K fixing F is determined by its restriction to such L, so the natural map is injective. On the other hand, it is clear from the definition of the inverse limit that if we have a system of automorphisms of every L/F compatible with restriction, that it induces a well-defined automorphism of K fixing F, so we have surjectivity as well. □

We immediately conclude:

Corollary 1.2. *If K/F is Galois, then* $\operatorname{Gal}(K/F)$ *naturally has the structure of a profinite group, induced by the isomorphism of the proposition.*

As a first example of an infinite Galois group, we consider finite fields.

Example 1.3. Let $\mathbb{F}_q$ be a finite field. Since finite fields are perfect, we see that $\bar{\mathbb{F}}_q$ is Galois over $\mathbb{F}_q$. We know that for every n, there is a unique extension of $\mathbb{F}_q$ of degree n, with Galois group canonically isomorphic to $\mathbb{Z}/n\mathbb{Z}$, and that the extension of degree m is contained in the extension of degree n if and only if $m|n$. This means that $\operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is the inverse limit over all positive n of $\mathbb{Z}/n\mathbb{Z}$, under the canonical quotient maps. By definition, this is $\hat{\mathbb{Z}}$, the free profinite group on one (topological) generator.

Since we have opened the door to infinite Galois extensions, it is natural to consider the maximal Galois group of any given field. If F is perfect, its maximal Galois group is $\operatorname{Gal}(\bar{F}/F)$. If not, $\bar{F}$ is not separable over F, so we need to consider a smaller field.

Definition 1.4. Given a field F, the **separable closure** F^{sep} of F is the separable part of the field extension $\bar{F}/F$. The **absolute Galois group** G_F of F is $\operatorname{Gal}(F^{\text{sep}}/F)$.

Note that the latter definition makes sense, since F^{sep} is always Galois over F. Indeed, if α is separable over F, all the other roots of its minimal polynomial over F are likewise separable, and therefore contained in F^{sep}.

2. The fundamental theorem

The extension of the fundamental theorem of Galois theory to arbitrary Galois extensions is the following:

Theorem 2.1. *Let K/F be a Galois extension, with $G := \mathrm{Gal}(K/F)$. Then the maps $L \mapsto \mathrm{Gal}(K/L)$ and $H \mapsto K^H$ are mutually inverse, inducing an inclusion-reversing bijection between fields L lying between K and F, and closed subgroups H of G.*

More precisely, we have for any intermediate field L that $K^{\mathrm{Gal}(K/L)} = L$, and for any subgroup $H \subseteq G$, that $\mathrm{Gal}(K/K^H) = \bar{H}$, where $\bar{H}$ is the closure of H in G.

Furthermore, under the given correspondence:

1. *finite extensions L/F correspond to open subgroups $H \subseteq G$, and indeed cosets of $H \subseteq G$ are in bijection with imbeddings of L into K fixing F;*
2. *Galois extensions L/F correspond to normal closed subgroups $H \trianglelefteq G$, and indeed conjugates of L correspond to conjugates of H;*

Note that (1) is the correct generalization to infinite extensions of the statement that the degree of L over F is the index of H in G. Before proving the theorem, we need two simple lemmas, the first on profinite groups and the second on normal extensions.

Lemma 2.2. *Let $G = \varprojlim_{i \in I} G_i$ be a profinite group, where the G_i are an inverse system of finite groups. Suppose $H \subseteq G$ is a subgroup. Then H is open in G if and only if there exists $i \in I$ and a subgroup $H_i \subseteq G_i$ such that H is the preimage of H_i under the projection map $G \to G_i$.*

Proof. Since the map $G \to G_i$ is ocntinuous and G_i has the discrete topology, the preimage in G of any subset of G_i is certainly open. Conversely, suppose H is open in G. Then we have seen that H is also closed, hence compact, so H is covered by a finite number of open sets of the form $H \cap \prod_{i \in I} U_i$, where $U_i = G_i$ for all but finitely many i. By the definition of inverse limits, each such set can actually be written with only a single $U_i \neq G_i$. Similarly, since H is a finite union of such sets, it can also be written in the same form, with a single $U_i \neq G_i$. That is to say, H is the preimage of U_i under $G \to G_i$. But since $G \to G_i$ is a group homomorphism, the image of H is a subgroup $H_i \subseteq G_i$, so we see that H is indeed the preimage of a subgroup H_i, as desired. □

The following lemma follows easily from our earlier results, and has been used implicitly before. We state it explicitly for the sake of clarity.

Lemma 2.3. *Suppose K/F is normal, and L is an intermediate extension. Then any imbedding $L \to \bar{K}$ fixing F has image contained in K, and can be extended to an automorphism of K fixing F.*

Proof. Indeed, since K/L is algebraic, any imbedding $L \to \bar{K}$ fixing F extends to an imbedding $K \to \bar{K}$ fixing F, which must have image K since K/F is normal. Thus, the image of L is contained in K, and moreover, the extended imbedding differs from the inclusion $K \subseteq \bar{K}$ by an automorphism of K, which necessarily fixes F. □

The main additional result on profinite groups we recall is that a subgroup is closed if and only if it is the intersection of open subgroups. Armed with our knowledge of profinite groups and the fundamental theorem of Galois theory in the finite case, it is now easy enough to prove the generalization.

Proof of theorem. We already proved in full generality that K/L is Galois if and only if $K^{\mathrm{Gal}(K/L)} = L$.

For the other direction, we first prove that $\mathrm{Gal}(K/K^H) = H$ when H is open. By Lemma 2.2, H is the preimage of some $H_L \subseteq \mathrm{Gal}(L/F)$ for L/F finite Galois, with $L \subseteq K$. That is, H is the set of automorphisms of K which restrict on L to an element of H_L. Now suppose $\sigma \in \mathrm{Gal}(K/K^H)$. Then σ fixes all the elements of L^{H_L}, since the definition makes it clear that $L^{H_L} \subseteq K^H$, so by the fundamental theorem of Galois theory applied in the finite case, σ restricts on L to an element of H_L, and we thus have $\sigma \in H$. Hence $\mathrm{Gal}(K/K^H) \subseteq H$, but the other inclusion is obvious, so we have proved the desired statement.

We next claim that for any $H \subseteq G$, we have that $\mathrm{Gal}(K/K^H)$ is closed. $\mathrm{Gal}(K/K^H)$ is clearly the intersection of $\mathrm{Gal}(K/L)$, where L/F is finite and $L \subseteq K^H$. For each such L, if E/F is the Galois closure, $\mathrm{Gal}(K/L)$ is the preimage in $\mathrm{Gal}(K/F)$ of the subgroup $\mathrm{Gal}(E/L) \subseteq \mathrm{Gal}(E/F)$, so is an open subgroup. Hence $\mathrm{Gal}(K/K^H)$ is closed. Since $H \subseteq \mathrm{Gal}(K/K^H)$, we have $\bar{H} \subseteq \mathrm{Gal}(K/K^H)$, and just need to prove equality.

We are therefore reduced to seeing that $\mathrm{Gal}(K/K^H) \subseteq H$ when H is closed. We know that H is the intersection of the open subgroups H' containing it, so let H' be an open subgroup containing H. Then certainly $K^{H'} \subseteq K^H$, so $\mathrm{Gal}(K/K^H) \subseteq \mathrm{Gal}(K/K^{H'}) = H'$ by the above, so we find $\mathrm{Gal}(K/K^H) \subseteq \cap_{H' \supseteq H \text{ open}} H' = H$, and we obtain the desired equality.

It remains to prove assertions (1) and (2). For (1), we first note that the second part implies the first: indeed, a closed subgroup is open if and only if it has finite index, and we claim that because L/F is separable, it has finitely many imbeddings in K fixing F if and only if it is finite over F. Certainly, if L/F is finite, it has finitely many imbeddings. Conversely, every imbedding of a subfield can be extended to all of L, and the extended imbedding has image contained in K by Lemma 2.3. If L/K is not finite, it contains finite extensions of arbitrarily large degree, which then produce arbitrarily many imbeddings.

Next, we see that for $\sigma \in G$, we obtain an imbedding $L \hookrightarrow K$ fixing F, simply by applying σ to the given inclusion $L \subseteq K$. Moreover, we obtain the same imbedding for any element in σH, since elements of H fix L, so precomposing by them doesn't change the imbeddings. We thus have a map from left cosets of H to imbeddings of L into K fixing F, and we wish to see this is surjective. But surjectivity follows immediately from Lemma 2.3.

Moving on to (2), we again start by observing that the second part implies the first. In this case, it suffices to see that a field extension L/F contained in K is normal if and only if $\sigma(L) = L$ for all $\sigma \in \mathrm{Gal}(K/F)$. But Lemma 2.3 implies that $\{\sigma(L) : \sigma \in \mathrm{Gal}(K/F)\}$ is precisely the set of images of imbeddings of L into $\bar{K}$ fixing F, so these are all equal precisely when L/F is normal.

Finally, we note that

$$\begin{aligned}K^{\sigma H\sigma^{-1}} &= \{x \in K : \forall \tau \in H, \sigma\tau\sigma^{-1}(x) = x\} \quad (y := \sigma^{-1}(x))\\ &= \sigma\{y \in K : \forall \tau \in H, \sigma\tau\sigma^{-1}(\sigma y) = \sigma y\}\\ &= \sigma\{y \in K : \forall \tau \in H, \tau(y) = y\}\\ &= \sigma K^H,\end{aligned}$$

and conversely

$$\begin{aligned}\mathrm{Gal}(K/\sigma(L)) &= \{\tau \in \mathrm{Gal}(K/F) : \forall x \in \sigma(L), \tau(x) = x\} \quad (y := \sigma^{-1}(x))\\ &= \{\tau \in \mathrm{Gal}(K/F) : \forall y \in L, \tau(\sigma(y)) = \sigma(y)\}\\ &= \{\tau \in \mathrm{Gal}(K/F) : \forall y \in L, \sigma^{-1}\tau\sigma(y) = y\} \quad (\xi := \sigma^{-1}\tau\sigma)\\ &= \sigma\{\xi \in \mathrm{Gal}(K/F) : \forall y \in L, \xi(y) = y\}\sigma^{-1}\\ &= \sigma\,\mathrm{Gal}(K/L)\sigma^{-1},\end{aligned}$$

so we obtain the desired bijection between conjugate fields of L and conjugate subgroups of H in $\mathrm{Gal}(K/F)$. □