

A Note About Profinite Groups

November 17, 2000

In this note we construct, for any profinite group G , a Galois extension K/F with $\text{Gal}(K/F) \cong G$. In addition, we give an example of a profinite group G that contains a normal subgroup of finite index that is not closed (or open). The following books are references for profinite groups and Galois theory: Shatz [3], Serre [2] and Morandi [1].

We recall the definition of an inverse limit along with some properties of profinite groups and facts of Galois theory. A *directed* set is a partially ordered set I such that for any $i, j \in I$, there is a k with $i \leq k$ and $j \leq k$. If I is a directed set, then a collection $\{G_i\}_{i \in I}$ of groups together with homomorphisms $f_{ij} : G_j \rightarrow G_i$ for each pair $i \leq j$ is an *inverse system* provided that $f_{ii} = \text{id}_{G_i}$ for each i , and whenever $i \leq j \leq k$, then $f_{ik} = f_{ij} \circ f_{jk}$. Finally, the *inverse limit* $\varprojlim G_i$ is a group G together with homomorphisms $f_i : G \rightarrow G_i$ with $f_j = f_{ij} \circ f_i$ for each pair $i \leq j$ that satisfies the following mapping property: given a group A and homomorphisms $\sigma_i : A \rightarrow G_i$ such that $\sigma_j = f_{ij} \circ \sigma_i$ for each $i \leq j$, then there is a unique homomorphism $\sigma : A \rightarrow G$ with $\sigma_i = f_i \circ \sigma$. An explicit construction of the inverse limit is

$$G = \{ \{g_k\} \in \prod_k G_k : g_i = f_{ij}(g_j) \text{ if } i \leq j \}$$

with the maps f_i the composition of the inclusion map $G \rightarrow \prod_k G_k$ with the projection map $\prod_k G_k \rightarrow G_i$. A simple consequence of the definition of an inverse limit is that if $G = \varprojlim G_i$, and if $f_i : G \rightarrow G_i$ is the given map, then $\{f_i(G)\}$ is an inverse system of groups and $G = \varprojlim f_i(G)$. Therefore, we may assume that each group in the inverse system $\{G_i\}$ is a homomorphic image of G .

A *profinite group* is an inverse limit of finite groups. Let $G = \varprojlim G_i$ be a profinite group. We view G as obtained by the construction above. If we put the discrete topology on each G_i , and the product topology on $\prod_i G_i$, then a short argument shows that G is a closed subspace of the product; in particular, G has a topology. Furthermore, G is compact and Hausdorff as a topological space. Moreover, the multiplication on G and the inversion map are continuous maps $G \times G \rightarrow G$ and $G \rightarrow G$. That is, G is a *topological group*. As a consequence, if $g \in G$, then the left multiplication map $x \mapsto gx$ is a homeomorphism of G . Similarly, right multiplication is a homeomorphism.

Let K/F be a Galois extension of fields of arbitrary degree, and let $G = \text{Gal}(K/F)$. If $\{L_i\}$ is the set of subfields of K that are finite dimensional Galois extensions of F , and if

$G_i = \text{Gal}(L_i/F)$, then the G_i form an inverse system of groups (with the obvious restriction of functions maps) and that $G = \varprojlim G_i$; see Section 17 of [1]. The generalized fundamental theorem of Galois theory states that there is a 1–1 inclusion reversing correspondence between intermediate fields of K/F and closed subgroups of $\text{Gal}(K/F)$. Furthermore, if $H \longleftrightarrow L$; that is, $H = \text{Gal}(K/L)$ and L is the fixed field of H , then $[L : F] = [G : H]$, and L/F is Galois if and only if H is normal in G . Furthermore, when this happens, $\text{Gal}(L/F) \cong G/H$. One important fact used to prove the fundamental theorem is the following description of the closure of a subgroup: if H is a subgroup of G , and if \overline{H} is the closure of H , then $\overline{H} = \text{Gal}(K/L)$ if L is the fixed field of H . This can be found in [1, Thm. 17.7].

The following lemma will aid us in constructing a Galois extension whose Galois group is a given profinite group.

Lemma 1. *Let $\{L_i\}_{i \in I}$ be a directed system of finite Galois extensions of a field F . If K is the composite of the L_i , then $\text{Gal}(K/F) = \varprojlim \text{Gal}(L_i/F)$.*

Proof. We may assume that the maps of the directed system $\{L_i\}$ are inclusions. Then K is in fact the union of the L_i . We first note that $\{\text{Gal}(L_i/F)\}_{i \in I}$ is an inverse system of groups, where the maps are defined as follows: if $i \leq j$, then $L_i \subseteq L_j$, and the map $f_{ij} : \text{Gal}(L_j/F) \rightarrow \text{Gal}(L_i/F)$ is given by $\sigma \mapsto \sigma|_{L_i}$. It is then trivial to check that this set of groups is an inverse system. To prove that $G := \text{Gal}(K/F)$ is the inverse limit of this system, we first note that there is a map $f_i : G \rightarrow \text{Gal}(L_i/F)$ given by $f_i(\sigma) = \sigma|_{L_i}$. To verify the claim, let A be a group, and, for each i , let $\varphi_i : A \rightarrow \text{Gal}(L_i/F)$ be a homomorphism such that $\varphi_j = \varphi_i \circ f_{ij}$ for each pair $i \leq j$. Then define $\varphi : A \rightarrow G$ as follows. If $a \in A$, let $\varphi(a) : K \rightarrow K$ be the automorphism whose restriction to L_i is $\varphi_i(a)$. This is well defined since the field K is the union of the L_i . The map φ is clearly the unique homomorphism satisfying $f_i \circ \varphi = \varphi_i$. This then proves that $G = \varprojlim \text{Gal}(L_i/F)$. \square

Proposition 2. *Let G be a profinite group. Then there is a Galois extension K/F with $\text{Gal}(K/F) \cong G$.*

Proof. Let k be a field, and let $M = k(\{x_g : g \in G\})$ be the rational function field over k in variables $\{x_g\}$, one variable for each element of G . Then G acts as a group of permutations on the variables via $g(x_h) = x_{gh}$. This action extends to an action of G as a group of automorphisms of M . It is clear that this action is faithful, since $g(x_h) = x_h$ implies that $x_{gh} = x_h$, so $gh = h$, and thus $g = 1$. Let F be the fixed field of G . We write $G = \varprojlim G_i$ for an inverse system of finite groups $\{G_i\}$; as noted earlier, we may assume that each G_i is a homomorphic image of G . So, write $G_i = G/N_i$ for some normal subgroup of finite index N_i . Let L_i be the fixed field of N_i . We first prove that L_i/F is a finite Galois extension with Galois group G_i . For ease of notation we write $N = N_i$ and $L = L_i$. Let $a \in L$. Then $g(a) \in L$ for any $g \in G$, since if $n \in N$, we have $g^{-1}ng \in N$, so $g^{-1}ng(a) = a$, or $ng(a) = g(a)$. Thus, $g(a)$ is in the fixed field of N ; that is, $g(a) \in L$. Next, we have a group homomorphism $G \rightarrow \text{Gal}(L/F)$ given by $g \mapsto g|_L$. This has kernel N , so G/N embeds in $\text{Gal}(L/F)$. Furthermore, the fixed field of G/N is F ; if $b \in L$ is fixed by all elements of

G/N , then $b \in M$ is fixed by all elements of G from the definition $(gN)(b) = g(b)$. Thus, $b \in F$. We now quote a theorem of Galois theory: if L is a field and if H is a finite group of automorphisms of L with fixed field H , then L/F is Galois and $H = \text{Gal}(L/F)$. Thus, in our case we also get $|G/N| = [L : F]$, so L/F is a finite Galois extension. These statements can be found in [1, Sec. 2]. We thus have a collection $\{L_i\}$ of Galois extensions of F with $\text{Gal}(L_i/F) = G/N_i$. Let K be the composite of the L_i . Then K/F is Galois. The previous lemma yields $\text{Gal}(K/F) = \varprojlim G/N_i = G$, as desired. \square

In the remainder of this note we work several exercises from [1], including disproving one of them. Notably, we construct a profinite group G that contains a normal subgroup of finite index that is neither open nor closed in the inverse limit topology of G . This gives a counterexample to Problem 7 in Appendix C of [1]. This example answers Problem 7 of Section 17. Note that the proposition above is exactly Problem 17 of Section 17.

Consider the following inverse system: choose a prime p and let $A_n = \bigoplus_{i=1}^n \mathbb{Z}_p$, and for $i \leq j$, let $\varphi_{ij} : A_j \rightarrow A_i$ be the map $\varphi_{ij}(x_1, \dots, x_j) = (x_1, \dots, x_i)$. We claim that $A := \varprojlim \mathbb{Z}_p$ is the inverse limit of this system. To prove this, we first define maps $\varphi_i : A \rightarrow A_i$ by $\varphi_i(\{x_k\}) = (x_1, \dots, x_i)$. Then it is clear that $\varphi_i = \varphi_{ij} \circ \varphi_j$ for all $i \leq j$. Next, suppose that B is a group and $f_i : B \rightarrow A_i$ is a homomorphism with $f_i = \varphi_{ij} \circ f_j$ for all $i \leq j$. We define $f : B \rightarrow A$ by $f(b) = \{x_k\}$ if $f_i(b) = (x_1, \dots, x_i)$. Note that this uniquely determines x_k for all $k \in \mathbb{N}$. This map is clearly the unique map satisfying $f_i = f \circ \varphi_i$. Thus, A is indeed the inverse limit of the $\{A_n\}$.

We now produce normal subgroups of finite index in G that are neither open nor closed. Recall that for a subgroup N of finite index, N is closed if and only if N is open. Let $\{x_\alpha\}_{\alpha \in \Gamma}$ be a basis for A . For each $\alpha \in \Gamma$, let H_α be the span of all of the basis vectors except x_α . Then $[A : H_\alpha] = p$, so H_α has finite index. Furthermore, H_α is normal since A is Abelian. Suppose that each H_α is open (and closed). It is clear from the definition of linear combination that $\bigcup_{\alpha \in \Gamma} H_\alpha = A$. Compactness of A then implies that a finite union $H_{\alpha_1} \cup \dots \cup H_{\alpha_n} = A$. However, this is false since $x_{\alpha_1} + \dots + x_{\alpha_n}$ is not in this union. Therefore, some H_α is not open. This verifies our claim.

As a consequence of this example, we see that if G is profinite, and if \widehat{G} is the inverse limit of all finite images of G , then there is a canonical homomorphism $f : G \rightarrow \widehat{G}$ arising from the mapping property for \widehat{G} . This map need not be an isomorphism of topological groups, since if N is normal subgroup of finite index, and $\varphi_N : \widehat{G} \rightarrow G/N$ is the map associated to G/N , then φ_N is continuous. If f was continuous, then $f^{-1}(\varphi_N^{-1}(0)) = N$ would be closed in G , which we now know is not always true.

References

- [1] P. J. Morandi, *Field and Galois Theory*, Graduate Texts in Mathematics, vol. 167, Springer, New York, 1996.

- [2] J.-P. Serre, *Cohomologie Galoisienne*, fifth ed., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin and Heidelberg and New York, 1994.
- [3] S. S. Shatz, *Profinite groups, arithmetic, and geometry*, Annals of Mathematics Studies, vol. 67, Princeton University Press, Princeton, NJ, 1972.