INFINITE GALOIS THEORY & PROFINITE GROUP TOPOLOGY

CINDY TSANG

Abstract: I will introduce the Krull topology that one can define on an infinite Galois group to obtain a similar correspondence theorem as in the finite case. I will also introduce the profinite group topology and explain how the Krull topology is a special case.

I. Infinite Galois Theory

Let K/F be a Galois extension of fields with Galois group $G = G(K/F)$.

If the extension is finite, then we know that there is a nice one-to-one correspondence between subgroups of G and intermediate extensions of K/F.

Fundamental Theorem of Finite Galois Theory. There is a one-to-one correspondence between subgroups of G and intermediate extensions of K/F, given by the maps

$$H \mapsto \mathcal{F}(H) \text{ and } L \mapsto G(K/L).$$

Futhermore, an intermediate extension L is Galois if and only the corresponding subgroup H is a normal subgroup of G.

But what if the extension is infinite? Do we still have this nice one-to-one correspondence? The answer is no because in general there are more subgroups than intermediate fields. However, it turns out that if we put the right topology on the group G, then we can get an analogous one-to-one correspondence between *closed* subgroups of G and intermediate extensions of K/F. We even get that an intermediate extension is *finite* if and only if the corresponding subgroup is *open*.

Fundamental Theorem of Infinite Galois Theory. There is a one-to-one correspondence between *closed* subgroups of G and intermediate extensions of K/F, given by the maps

$$H \mapsto \mathcal{F}(H) \text{ and } L \mapsto G(K/L).$$

Furthermore, an intermediate extension L is Galois if and only if the corresponding subgroup H is a normal subgroup of G; and $[L : F]$ is *finite* if and only if $[G : H]$ is *finite* and if and only if H is *open*.

Although this is called Fundamental Theorem of Infinite Galois Theory, it is actually only a generalization of the finite case because the topology turns out to be discrete when K/F is finite.

II. Krull Topology

So how do we define a topology on G to make this work? We are going to specify what the basis is. In particular, we want the topology to be generated by the basis

$$\mathcal{B} = \{\sigma H : \sigma \in G,\ H = G(K/E),\ E/F \text{ finite}\}.$$

If K/F is finite then we can take $E = K$. In that case H is the trivial group so we get that every $\sigma \in G$ is in the basis. So we get the discrete topology in the finite case, as mentioned before.

Observations.

1) Every element in $\mathcal{B}$ is a clopen set: Since

$$G(E/F) \simeq \frac{G(K/F)}{G(K/E)} := \frac{G}{H}$$

(we know this is true when K/F is finite but the infinite case isn't exactly the same; so this requires a proof but I am going to skip it here), if E/F is finite then $[G : H]$ is finite also. Hence, there exists $\sigma_1, ..., \sigma_n \in G$ such that

$$G = \bigsqcup_{i=1}^{n} \sigma_i H.$$

Since σH is one of them and the union is disjoint, clearly σH is also a closed set.

2) The collection $\mathcal{B}$ is indeed a basis:

a. Take $E = F$ above and we see that $\mathcal{B}$ covers the entire space G.

b. Let $H_1 = G(K/E_1)$ and $H_2 = G(K/E_2)$, where E_1, E_2 are finite extensions of F. Then, E_1E_2 is finite over F and $H_1 \cap H_2 = G(K/E_1E_2)$ (this is obvious).

III. Profinite groups

The Krull topology can actually be realized as a profinite group topology. Essentially a profinite group is built out of finite groups. Let me explain what a it is and the natural topology we can put on it.

Definition. Let A is a partially ordered set. A family $\{G_a, \phi_{b,a}\}$ is called a *projective family* if

1) $\phi_{b,a} : G_b \to G_a$ is a group homomorphism $(a \leq b)$;
2) $\phi_{a,a} : G_a \to G_a$ is identity on G_a;
3) $\phi_{b,a} \circ \phi_{c,b} = \phi_{c,a}$ whenever $a \leq b \leq c$.

We can view ordering as describing when a group G_b lies above another group G_a $(a \leq b)$ and the $\phi_{b,a}$ as projections onto the group lying below. Then 2) says we must have the identity map when projecting onto the same group; and 3) says we can project from G_c to G_b then to G_a or directly from G_c to G_a, and the results are the same.

Definition. A group $\overline{G}$ is a *profinite group* if $\overline{G} = \varprojlim G_a$ for a projective family $\{G_a, \phi_{b,a}\}$, where each G_a is a finite group. The notation $\varprojlim G_a$ represents the *projective limit* (also called *inverse limit*) of $\{G_a, \phi_{b,a}\}$ and is defined by

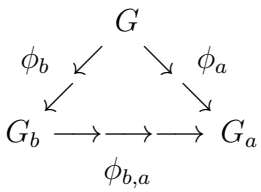
$$\varprojlim G_a = \{(g_a)_{a\in A} \in \prod_{a\in A} G_a |\ \phi_{b,a}(g_b) = g_a\ \forall a \leq b\},$$

and the natural *profinite group topology* is simply

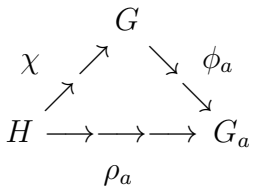
$$G_a \text{ discrete topology} \to \prod_{a\in A} G_a \text{ product topology} \to \varprojlim G_a \text{ subspace topology}.$$

It turns out the $\overline{G}$ is always a closed subspace of the product space $\prod G_a$.

We can think of the projective limit as a way to piece the smaller groups G_a together and it naturally lies above all of them. In particular, for each G_a there is a natural projection map $\phi_a : G \to G_a$. We want this extra condition $\phi_{b,a}(g_b) = g_a$ because we want to be able to project from G to G_b then to G_a, or directly from G to G_a, and get the same result either way. That is, we want the following diagram to commute:



Furthermore, if $\rho_a : H \to G_a$ has the same property, we want to be able to piece these maps together to get a unique homomorphism from H to G. That is, we want there to exist a unique group homomorphism $\chi : H \to G$ so that the following diagram commutes:



This is actually another definition of profinite group by means of a univeral property.

Example. If we consider the projection family of $\mathbb{Z}/p^n\mathbb{Z}$ with the usual projective map,

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \leftarrow \frac{\mathbb{Z}}{p^2\mathbb{Z}} \leftarrow \frac{\mathbb{Z}}{p^3\mathbb{Z}} \leftarrow \cdots \leftarrow \cdots$$

then the projective limit gives us the p-adic integers. This is one of the common ways to define $\mathbb{Z}_p$ other than the series representation.

IV. Krull topology on $G = G(K/F)$ as a profinite group topology

Now back to Krull topology. How do we define it as a profinite group? There is only one natural thing to do. We want a family of finite groups, so the only thing we have is the finite Galois groups, and the natural way to order them is by inclusion of the corresponding fields. More precisely, this is what we are going to do.

Partially order the set

$$I = \{E : E \text{ finite intermediate extension of } K/F\}$$

by inclusion. For $L \subset E$ define

$$\phi_{E,L} : G(E/F) \to G(L/F) \text{ by letting } \sigma \mapsto \sigma|_L.$$

Then we obtain a projective family

$$(G(E/F), \phi_{E,L})_{E \in I}.$$

Theorem. The topological groups $\varprojlim G(E/F)$ and G are homeomorphic under the map

$$\chi : G \to \varprojlim G(E/F) \text{ defined by } \sigma \mapsto (\sigma|_E)_{E \in I}.$$

Notice that χ is a group homomorphism also since restriction and composition of maps commute.

Proof. It is very easy to prove that χ is injective. For if $\sigma|_E = \mathrm{id}_E$ for all finite extensions E/F, then given any $\alpha \in K$ we can take $E = K(\alpha)$, which is finite because α is algebraic, we immediately see that $\sigma(\alpha) = \alpha$ and so $\sigma = \mathrm{id}_K$.

V. Other characterizations of profinite group topology

It is amazing that every Galois group can be realized as a profinite group. What is even more cool is the converse is actually true: every profinite group is the Galois group of some field extension. In fact, we can even characterize a profinite or Galois group topologically by specifying that it is compact, Hausdorff, and totally disconnected.

Theorem. Let T be a topological group. The following are equivalent:

1) T is the Galois group of some field extension.
2) T is a profinite group.
3) T is compact, Hausdorff, and totally disconnected.

Proof. The implication 2) $\implies$ 3) is actually quite easy to prove if we assume that the fact that projective limit is a closed subspace of the product space and use some basic facts from topology. So let $T = \varprojlim G_a$ be a profinite group.

a. T is compact: Each G_a is compact because it is finite. Product of compact spaces is again compact by Tychanoff theorem. A closed subspace of a compact space is again compact.

b. T is Hausdorff: Each G_a is Hausdorff because it has the discrete topology. Product of Hausdorff spaces is Hausdorff and a subspace of a Hausdorff space is again Hausdorff.

c. T is totally disconencted: Each G_a is totally disconnected because it has the discrete topology. Product of totally disconnected spaces is totally disconnected and a subspace of a totally disconnected space is again totally disconnected.

The materials here are based on:

1) Frederick Butler's thesis "Infinite Galois Theory".
http://faculty.ycp.edu/~fbutler/MastersThesis.pdf