GALOIS EXTENSIONS

ZIJIAN YAO

This is a basic treatment on infinite Galois extensions, here we give necessary backgrounds for Krull topology, and describe the infinite Galois correspondence, namely, sub-extensions correspond to closed subgroups in a $1-1$ fashion. In addition, sub-extensions of finite degree correspond to open subgroups. We follow Neukirch and professor Abramovich's lecture notes. The author is responsible for all potential mistakes, since some of the arguments are not referred to any literature.

1. Topological Groups

First we discuss topological groups.

Definition. A topological group is a group G with a topology such that both multiplication and taking inverses are continuous. Namely, the maps

$$(g,h) \mapsto gh, \qquad g \mapsto g^{-1}$$

are continuos.

Remark. From the definition it is clear that left multiplication is continuous, since $L_a : G \to G$ is given by $g \mapsto ag$, and can be written as $G \xrightarrow{g\mapsto(a,g)} G \times G \xrightarrow{(g,h)\mapsto gh} G$. In fact, L_a is a homeomorphism with inverse $L_{a^{-1}}$.

Lemma 1.1. Let $H < G$ be a subgroup, then

- H is open $\Rightarrow$ H is closed.
- H is closed of finite index $\Rightarrow$ H is open.

  However, H is closed does NOT imply it is open.

Proof. Let $S = G/H$ be a set of representatives of cosets of H, then $G\backslash H = \bigcup_{\sigma\in S\backslash\{e\}} \sigma H$, so both claims follow directly.

□

Remark. Recall the definition of neighbourhood base (or nbhd system) at $x \in X$ is a set of neighbourhoods $\mathcal{M}$ such that every open neighbourhood U of x contains some $M \in \mathcal{M}$.

Neighbourhood systems in topological groups are nice. In fact, topological groups are very very nice in general.

Date: Fall 2014.

2. Galois group and inverse limit

Let us fix a (possibly) infinite Galois extension K/k and let $G = Gal(K/k)$. Let F/k be a finite sub-extension of K such that F/k is Galois. So K/F and F/k are both Galois. Let $H = Gal(K/F)$, then $H \lhd G$ and $G(F/k) \cong G/H$. In particular, since F/k is finite, H is of finite index in G. We have a canonical homomorphism

$$G \to G/H = G(F/k) \qquad \text{by } \sigma \mapsto \sigma|_F$$

for each $H = G(K/F)$. Therefore, we have a homomorphism from G to the inverse limit of the (inversely) directed family of normal subgroups with finite index:

$$\varphi : G \to \lim_{H \in \mathcal{F}} G/H$$

where $\mathcal{F}$ is the family of Galois groups as above.

Proposition 2.1. *The homomorphism $\varphi : G \to \lim_{H\in\mathcal{F}} G/H$ is an isomorphism.*

Proof. The map is obviously injective. For surjectivity, start from $\{\sigma_F\} \in \lim G/H = \lim G(F/k)$, pick any $\alpha \in K$, choose $\alpha \in E/k$ and define $\sigma(\alpha) = \sigma_E(\alpha)$. The map is clearly well-defined and lies in G.

□

3. The Krull topology

Now we want to describe the Galois correspondence. This is done by giving the Galois group G a topology, called the Krull topology. Under this topology, we will establish $1-1$ correspondence of intermediate extensions of K/k with closed subgroups of G.

Definition. The Krull topology is defined as follows: for each F finite Galois sub-extension of K, we give the Galois group $G(F/k) = G/H$ the discrete topology, and the product $\prod G/H$ the product topology, or the Tychonoff topology. We embed $G \cong \lim G/H$ into $\prod G/H$, and give it the induced subset topology, this is what we call the Krull topology on G. Note that the topology on G is the one that forces the map φ to be a homeomorphism.

Definition. We define a topology on G, for now called *topology 1*, as follows: for each $\sigma \in G$, let $\sigma H = \sigma G(G/F)$ where $F \in \mathcal{F}$ be a basis for $\sigma \in G$.

Remark. It is easy to check that this indeed defines a basis, thus a topology on G.

Proposition 3.1. *Under this topology, G is a topological group, namely, both the multiplication map and the inverse map are continuous.*

Proof. This follows immediately from definition. □

Proposition 3.2. *Topology* 1 *and the Krull topology coincide on $G = G(K/k)$.*

Proof. Note that the basis for $\prod G/H$ is $\{\prod_{H\neq H_o} G/H \times \{\bar{\sigma}\}\}$ where $H_0 = G(K/F_0)$ ranges over all finite Galois sub-extensions of K, and $\bar{\sigma} \in G(F_0/k) = G/H_0$. Consider the injection $\psi : G \to \prod G/H$. Let $\sigma \in G$ and U_0 be a basis of the above form, then $\psi^{-1}(U_0) = \sigma H_0$. □

Corollary 3.3. G is a topological group under the Krull topology.

Theorem 3.4. *G is compact Hausdorff and totally disconnected.*

Remark. This is in fact a characterization of profinite groups.

Proof.

(1). Hausdorff is obvious.

(2). We want to show G is compact. Note that each G/H is finite, hence compact, so $\prod G/H$ is compact, and it suffices to show that $G \cong \lim G/H$ is closed in $\prod G/H$. For each pair of finite Galois sub-extensions L, L' such that $L'/L/k$, we consider the set

$$S_{L'/L} = \{(\sigma_F) \in \prod G(F/k) : (\sigma_{L'})|_L = \sigma_L\}.$$

Note that $S_{L'/L}$ is closed, for the following reason: let $G(L/k) = \{\sigma_1, ..., \sigma_n\}$, and $S_i \subset G(L'/k)$ be the subset of $G(L'/k)$ extending σ_i for each i, so S_i is finite. It is clear that $S_{L'/L} = \bigcup_{i=1,...,n}(\prod_{F\neq L',L} G(F/k) \times S_i \times \{\sigma_i\})$, which is closed in the product topology.

Therefore $\lim G/H = \lim G(F/k) = \bigcap_{L'/L} S_{L'/L}$ is closed.

(3). This is also obvious from construction.

□

There is yet another topology we can define on $G \cong \lim G/H$, which is essentially the compact-open topology. We will show that this again defines the same topology as the Krull topology.

Definition. We define another topology, called *Topology 2* on G as follows: regard $G = G(K/k) \subset K^K = \prod_{\alpha\in K} K$, and for each copy of K, we use the co-finite topology, i.e., finite subsets are closed.

Proposition 3.5. *Topology* 2 *and the Krull topology coincide on $G = G(K/k)$.*

Proof. The closed sets in the product topology $\prod_{\alpha\in K} K$ is given by

$$Y_{\alpha,\beta} = \{\sigma : \sigma(\alpha) = \beta\} \subset K^K,$$

while closed subsets in the Krull topology are generated by

$$X_{F,\bar{\sigma}} = \{\sigma : \sigma|_F = \bar{\sigma}\}$$

where $\bar{\sigma} \in G(F/k)$. Note that one is finite union of the other, therefore done.

□

4. Infinite Galois correspondence

Proposition 4.1. *Let M be a subfield of K over k, then the Galois group $G(K/M)$ is closed in G.*

Proof. We give two proofs, using topology 1 and 2 respectively.

(1). Take topology 1, we know that

$$G(K/M) = \bigcap_{M/F} G(K/F)$$

where F ranges over all finite sub-extensions (not necessarily Galois over k). Note that each $G(K/F)$ is open, hence closed, by considering neighbourhoods at each point. This shows that $G(K/M)$ is closed, since it is intersection of closed subsets.

(2). Another way to show this is using Topology 2, since $G(K/M) = \bigcap_{\alpha \in M} Y_{\alpha,\alpha}$.

□

Proposition 4.2. *Let H be any subgroup of G, then $G(K/K^H)$ is the closure of H.*

Proof. It is clear that $\overline{H} \subset G(K/K^H)$.

Now we want to show that, for any $\sigma \in G \backslash \overline{H}$, σ has to move some element in K^H. Note that $\sigma \notin \overline{H}$, therefore, we have

$$\sigma G(K/E) \cap H = \emptyset$$

for some E/k finite Galois.

Now consider

$$\phi : G(K/k) \to G(E/k)$$

and the image of H is restriction of elements in H to sub-extension E. Note that $\phi(\sigma) = \sigma|_E$ cannot lie in $\phi(H)$. Therefore, σ moves some element in $E^{\phi(H)} \subset K^H$. This proves that

$$G(K/K^H) = \overline{H}.$$

□

Proposition 4.3. *Let G be a compact topological group, then a subgroup $H < G$ is open if and only if H is closed of finite index.*

Proof. If H is closed of finite index, then it is obviously open (and this direction does not require compactness).Now assume H is open, and G is compact. Let $S = G/H$ be a set of representatives of cosets of H, then $\{\sigma H\}_{\sigma \in S}$ forms a disjoint open cover of G. By compactness, we know that H has finite index.

□

Theorem 4.4. *This is simply a remark/summary that we have proved the infinite Galois correspondence! Namely there is* $1-1$ *correspondence (by taking fixed field, Galois group, respective):*

$$\{\textit{Intermediate extensions } M \textit{ of } K/k\} \longleftrightarrow \{\textit{Closed subgroups of } G\}$$

$$\{\textit{Intermediate extension } M \textit{ of finite degree}\} \longleftrightarrow \{\textit{Open subgroups of } G\}$$

The rest of the correspondence (order reversing, taking conjugates, etc) is the same as in the finite case. See Lang, for example.

5. Some examples

Example. Let $\mu[p^\infty]$ be the union of all groups of roots of unity $\mu[p^n]$, where p is prime. We know that $(\mathbb{Z}/p^n\mathbb{Z})^* \cong G(\mathbb{Q}(\mu[p^n])/\mathbb{Q})$. The isomorphism is compatible in the tower of $p^t h$ roots of unity, so we take the inverse limit and get

$$\mathbb{Z}_p^* \cong G(\mathbb{Q}(\mu[p^\infty])/\mathbb{Q})$$

Example. Let $\mathbb{F}_p$ be a finite field where p is prime, then exists a unique extension of degree n for each n, namely the finite field $\mathbb{F}_{p^n}$. We know that $G(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$, generated by Frobenius. We from the inversely directed system for $\mathbb{Z}$ by division (which corresponds to taking extensions of fields). Again, the isomorphism is compatible with the directed system, and we have

$$G(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \lim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p.$$