Notes from the 2/24/23 talk by Cordell Smith

The Topological Constructions of Infinite Galois Groups and Profinite Groups

Note: This talk covers roughly pages 12-15 in Szamuely's Galois Groups and Fundamental Groups, the main reference for this course. However, these pages are quite terse and give little detail about how the topology of infinite Galois groups (and profinite groups in general) actually works. Therefore, I would recommend looking at pages 142-153 in Bosch's From the Viewpoint of Galois Theory. This talk will cover roughly pages 142-147 from that text. For an overview of the basic topological ideas covered in this talk, look at Leinster's General Topology, especially sections A2 and B1. This talk will present a synthesis of the information in all of these texts.

Review: Topology ≠ Metric Space Topology

Def: For a set X, a topology on X is a collection $\mathcal{T}$ of subsets of X called open subsets. Both X and $(X, \mathcal{T})$ are sometimes called topological spaces. The open subsets of X in $\mathcal{T}$ must have the following properties:

(1) For any family of subsets $(U_i)_{i\in I}$ such that $U_i \in \mathcal{T}$, $\forall i \in I$, $\bigcup_{i\in I} U_i \in \mathcal{T}$ (i.e. arbitrary unions of open subsets are open, arbitrary meaning finitely or infinitely many)

(2) For $U_1, U_2 \in \mathcal{T}$, $U_1 \cap U_2$ (i.e. finite intersections of open subsets are open.

(3) $\emptyset \in \mathcal{T}$ and $X \in \mathcal{T}$ (i.e. the empty set and the set X are open)

These are the axioms for the open subsets of X.

Topology:

Def: For $X(=(X, \mathcal{T}))$ a topological space and $x \in X$, an open neighborhood of x is an open subset of X containing x.

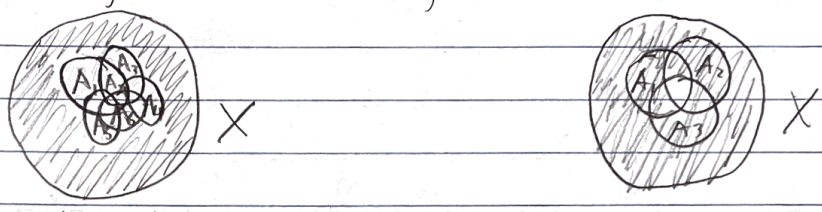
Def: For a topological space X, a subset $V \subseteq X$ is a closed subset of X if $X \setminus V \in \mathcal{T}$ (i.e. if the complement

of V in X is open)

Lemma: (De Morgan's Laws) A family $(A_i)_{i\in I}$ of subsets of X is a set I together with a subset $A_i \subseteq X$ for each $i \in I$.

(1) $X \setminus \bigcup_{i\in I} A_i = \bigcap_{i\in I} (X \setminus A_i)$ (2) $X \setminus \bigcap_{i\in I} A_i = \bigcup_{i\in I} (X \setminus A_i)$

Intuition: This proof comes from set theory and will be omitted. However, for intuition,



Thm: For a topological space X,

(1) For a family $(V_i)_{i\in I}$ of closed subsets of X, $\bigcap_{i\in I} V_i$ is closed in X (i.e. arbitrary intersections of closed subsets of X must be closed in X)

(2) For V_1, V_2 closed subsets of X, $V_1 \cup V_2$ is also closed in X (i.e. finite unions of closed subsets are closed)

(3) $\emptyset$ and X are closed subsets of X.

Proof: (1) $V_i = X \setminus A_i$ for some open A_i

$\bigcap_{i\in I}(X \setminus A_i) = X \setminus \bigcup_{i\in I} A_i$

$\bigcup_{i\in I} A_i$ must be open as a union of open sets

$\Rightarrow \bigcap_{i\in I}(X \setminus A_i) = \bigcap_{i\in I} V_i$ must be closed in X

(2) $V_1 = X \setminus A_1$; $V_2 = X \setminus A_2$

$\bigcup_{i\in\{1,2\}}(X \setminus A_i) = X \setminus \bigcap_{i\in\{1,2\}} A_i$

As we know $A_1 \cap A_2$ must be open, $X \setminus (A_1 \cap A_2)$ must be closed.

Therefore, $(X \setminus A_1) \cup (X \setminus A_2) = V_1 \cup V_2$ must be closed.

(3) $\emptyset$ and X are open, so $X \setminus \emptyset = X$ and $X \setminus X = \emptyset$ must be closed.

Remark: Notice that arbitrary intersections and finite unions of closed sets must be closed, as opposed to arbitrary unions and finite intersections of open sets being open.

Remark: This idea of a topology can be applied to any arbitrary set T of subsets of X, so long as it fulfills the properties required of an open set.

Def: The product of a family of topological spaces $(X_i)_{i\in I}$ is generated by all subsets of $\prod_{i\in I} U_i$ where U_i is open in X and $U_i = X_i$ for all but finitely many U_i

Def: A topology X is generated by a system B containing $\emptyset$, X and all finite intersections of all subsets of B (itself). A subset U of (X, T) is open $\Leftrightarrow U \in B$ or U is a union of sets belonging to B.

Note: These definitions come from Bosch, not Leinster.

Ex: For a set X, $\{\emptyset, X\} = B$ gives us $T = \{\emptyset, X\}$

Ex: For a set X and 2 elements $x_1, x_2 \in X$, $B = \{\emptyset, x_1, x_2, X\}$ for $x_1 \neq x_2$. Therefore, $T = \{\emptyset, x_1, x_2, x_1 \cup x_2, X\}$
Closed subsets: $\{\emptyset, X \setminus x_1, X \setminus x_2, X \setminus (x_1 \cup x_2), X\}$
However, most topologies we study are significantly more complicated

Remark: For this definition of topology, the set X can be pretty much whatever we want. In other words, X can have a structure outside of being a topological space.

Remark: In this topology, a subset $S \subseteq X$ can be open, closed, both open and closed, or neither open nor closed.

We now turn our attention to the infinite Galois extension L/k, as well as the system $S = (L_i)_{i\in I}$ of all subextensions of L/k which are both finite and Galois over K.

Def: The restriction of a topology on a set X to a subset $V \subset X$ is the topology on V whose open sets consist of the intersections of open sets U with V (i.e. $U \cap V$)
This topology is also referred to as the topology induced from X onto V (or simply the induced topology)
For any L_i a subfield of L such that L_i/k is Galois

and L_i is a finite extension of K, we can take the restriction homomorphism $f_i: Gal(L/K) \to Gal(L_i/K)$

Def: The discrete topology on X is the topology in which every subset of X is open (and therefore also closed).

Right now, it seems this topology will not give us much information

However, if we give the discrete topology to $Gal(L_i/K)$, we can take the inverse restriction maps f_i^{-1} and say that the topology we want to define on $Gal(L/K)$ is generated by the preimages $f_i^{-1}(\sigma)$ of points $\sigma \in Gal(L_i/K)$ for maps $f_i: Gal(L/K) \to Gal(L_i/K)$

This topology is sometimes called the Krull Topology

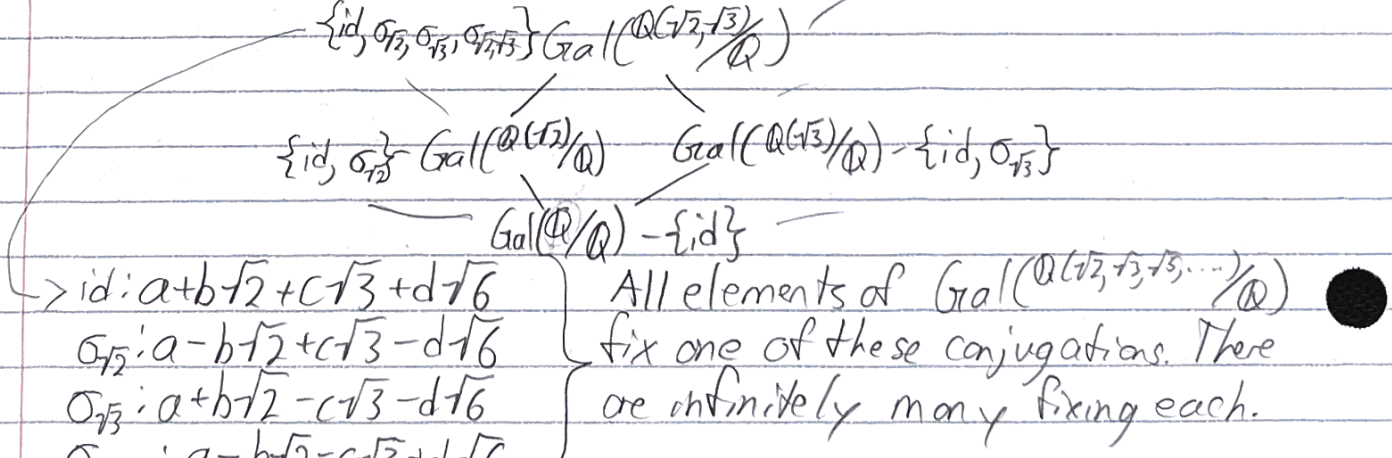
Why This One? Each $\sigma \in Gal(L_i/K)$ defines a specific automorphism of L_i. There are infinitely many automorphisms of L which are effectively extensions of σ. For all $\sigma' \in Gal(L/K)$, $\sigma(\alpha) = \sigma'(\alpha)$ if $\alpha \in L_i$. These open sets are therefore the set of all such σ' for each $\sigma \in Gal(L_i/K)$ for each $i \in I$, as well as unions for multiple such σ and intersections between σ.

This helps us visualize infinite Galois groups.

One more reason. . . . (will be discussed later)

Remark: Though $Gal(L/K)$ is infinite, it is still a group of automorphisms σ of L fixing all elements of K.

Ex: $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \ldots)/\mathbb{Q}$



- $id: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$
- $\sigma_{\sqrt{2}}: a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$
- $\sigma_{\sqrt{3}}: a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$
- $\sigma_{\sqrt{2},\sqrt{3}}: a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$

All elements of $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\ldots)/\mathbb{Q})$ fix one of these conjugations. There are infinitely many fixing each.

Lemmas: (1) A subset $U \subset Gal(L/K)$ is open $\Leftrightarrow \forall \sigma \in U: \exists i \in I$ such that $f_i^{-1}(f_i(\sigma)) \subset U$

(2) A subset $A \subset Gal(L/K)$ is closed $\Leftrightarrow \forall \sigma \in Gal(L/K)$ such that σ does not belong to A, $\exists i \in I: f_i^{-1}(f_i(\sigma)) \cap A = \emptyset$

(3) For a subset $D \subset Gal(L/K)$, its closure $\overline{D}$ consists of all $\sigma \in Gal(L/K)$ such that $f_i^{-1}(f_i(\sigma)) \cap D \neq \emptyset \ \forall i \in I$

Def: For a topological space X and $A \subseteq X$, the closure $\overline{A}$ of A is the intersection of all the closed subsets of X containing A. This is also the smallest closed subset containing A.

Intuition: The proofs will be omitted in full. (The proof of (1) is in Bosch.

But we can gain an intuition that if U is open, there must be some conjugation σ' or set of conjugations $\{\sigma_1', \ldots \sigma_n'\}$ such that $U = f_i^{-1}(\sigma')$ or $U = f_i^{-1}(\sigma_1') \cup f_i^{-1}(\sigma_2') \ldots$

So such an index I must exist $\forall \sigma \in U$

(1) Follows easily as we know $X \setminus A$ is open, so $\exists i \in I: f_i^{-1}(f_i(\sigma)) \in (X \setminus A) \Rightarrow f_i^{-1}(f_i(\sigma)) \notin A$

(3) Is a bit trickier, but it follows from (2) and the definition of the closure, as if an element $\sigma \in Gal(L/K)$ is not in some closed set containing D, $\exists i \in I: f_i^{-1}(f_i(\sigma)) \cap A = \emptyset$

So an element must be in the closure $\Leftrightarrow \forall i \in I: f_i^{-1}(f_i(\sigma)) \cap D \neq \emptyset$

Lemma: A set $A \subset X$ is closed $\Leftrightarrow$ for each $x \in X$, $x \notin A$, there exists an open neighborhood around x.

Proof: $\Rightarrow$ The complement of A is open, and this serves as the open neighborhood around x in A.

$\Leftarrow$ We know the union of all these open neighborhoods contains all $x \in X$, $x \notin A$, so this union is A^C and is open. Therefore $X \setminus A^C = A$ is closed

Remark: These statements show $Gal(L/K)$ is a topological group: a group G with a topology such that $G \times G \to G$ and $G \to G$ are continuous (i.e. preimages of open sets are open)

Def: For a topological space X, a cover of X is a family $(U_i)_{i\in I}$ of subsets of X such that $\bigcup_{i\in I} U_i = X$
Such a cover is finite if the indexing set I is finite (i.e. if there are a finite number of subsets in the family) and open if each U_i is open

Def: A topological space X is compact if every open cover of X has a finite open cover.

Def: Given a cover $(U_i)_{i\in I}$ and $J \subseteq I$, $(U_j)_{j\in J}$ is a subcover of $(U_i)_{i\in I}$ if it is itself a cover of X

Note: Bosch defines compactness a bit differently

Remark: These definitions look similar to those in metric space topology. However, they must be reevaluated in light of a new, more arbitrary definition of an open set.

Lemma: (Tychonoff's Theorem): The product of a collection of compact topological spaces is compact with respect to the product topology. This may be a finite or infinite collection.

Remark: Many proofs of this theorem exist, but they are long and/or build off nontrivial foundations

Thm: The topological group $Gal(L/K)$ is compact and totally disconnected

Def: A topological space X is totally disconnected if for every subset $A \subset X$ containing at least two points, there exist two open subsets $U, V \subset X$ such that $A \subset U \cup V$ as well as $U \cap A \neq \emptyset \neq V \cap A$ and $U \cap A \cap V = \emptyset$

Proof: The restriction maps $f_i : Gal(L/K) \to Gal(L_i/K)$ induce an injective homomorphism: $Gal(L/K) \hookrightarrow \prod_{i\in I} Gal(L_i/K)$ which we view as an inclusion
We know each $Gal(L_i/K)$ is a finite discrete topological space, so each $Gal(L_i/K)$ is compact.
Therefore $\prod_{i\in I} Gal(L_i/K)$ is compact by Tychonoff's Theorem

Remark: We can view $Gal(L/K)$ as a closed subset of $\prod_{i\in I} Gal(L_i/K)$, the product topology of the discrete

topology over each $Gal(L_i/K)$, equipped with the induced topology.

Lemma: Closed subspaces of compact spaces are compact.

Proof: Let $V \subset X$ with V closed.
Let $(U_i)_{i\in I}$ be a cover of V by open subsets of X.
As X is compact, it must have some finite subcover $(\bigcup_{j\in J} U_j)$
and as V is closed, $X \setminus V$ is open.
$(\bigcup_{j\in J} U_j) \cup (X \setminus V) = X$ So $\bigcup_{j\in J} U_j \supseteq V$ so V is compact
We now seek to show $Gal(L/K)$ is closed in $\prod Gal(L_i/K)$
Consider $(\sigma_i) \in \prod Gal(L_i/K)$ $(\sigma_i) \notin Gal(L/K)$
i.e. $\exists j, j' \in I : L_j \subset L_{j'}$ but $g(\sigma_{j'}) \neq \sigma_j$
where $g : Gal(L_{j'}/K) \to Gal(L_j/K)$
Therefore, the set of $(\sigma_i) \in \prod Gal(L_i/K)$ such that the element of L_j is σ_j and the element of $L_{j'}$ form an open neighborhood of σ_j which has no elements in $Gal(L/K)$
Think of $Gal(L/K)$ as a set of paths branching up towards some finer and finer automorphism
However, we are looking at this picture of branching paths from the opposite direction.
Essentially, we are looking at the subset of elements of $\prod Gal(L_i/K)$ where $g : Gal(L_{j'}/K) \to Gal(L_j/K)$, $g(\sigma_{j'}) = \sigma_k$ but $f_j(\sigma_k) \neq f_j(\sigma_{j'})$
This proves $Gal(L/K)$ is closed in L and therefore compact

Remark: We can extend this idea to say that the inverse limit $\varprojlim G_\alpha$ of any inverse system is a closed topological subgroup of the product $\prod G_\alpha$.

Proof: For $g \in \prod G_\alpha$, $g \notin \varprojlim G_\alpha$, we assume $\phi_{\alpha\beta}(g_\beta) \neq g_\alpha$
If we take an ordering of the inverse system, we can take the subset of $\prod G_\alpha$ whose component α is g_α and whose component β is g_β. These are open by the discreteness of G_α and the definition of a topological product.
As each $g \notin \varprojlim G_\alpha$ has such an open neighborhood, $\varprojlim G_\alpha$ must be closed

Remark: In fact, assuming the groups G_α are finite, $\prod G_\alpha$ must be

compact, so the above remark implies that all profinite groups are compact

Proof(cont): It suffices to show $\prod_{i\in I} Gal(L_i/K)$ is totally disconnected. For two elements $\sigma_j, \sigma_j' \in \prod_{i\in I} Gal(L_i/K)$, $\exists j \in I : \sigma_j \neq \sigma_j'$ and $\exists$ open subsets $V = \prod V_i$ and $V' = \prod V_i'$ in $Gal(L_i/K)$ defined by:

$$V_i = \begin{cases} Gal(L_i/K) & \text{for } i \neq j \\ \{\sigma_j\} & \text{for } i = j \end{cases} \qquad V_i' = \begin{cases} Gal(L_i/K) & \text{for } i \neq j \\ Gal(L_j/K) - \{\sigma_j\} & \text{for } i = j \end{cases}$$

Here we have $(\sigma_i) \in V$, $(\sigma_i') \in V'$ and $\prod Gal(L_i/K) = V \cup V'$ and $V \cap V' = \emptyset$

So any set containing at least 2 elements of $\prod Gal(L_i/K)$ is totally disconnected, and therefore $Gal(L/K)$ is totally disconnected.

Remark: A similar argument shows that any profinite group is totally disconnected. In effect, we take arbitrary G_i in place of $Gal(L_i/K)$ and arbitrary $\alpha, \alpha' \in \prod_{i\in I} G_i$

Thm: The open subgroups of a profinite group are the closed subgroups of finite index

Proof: (i) First, we show open subgroups are closed:

Fact: If U is a subgroup of a group G, then G is the disjoint union of its cosets gU. This comes from Modern Algebra I. In particular, the coset $eU = U$ is the complement of $\bigcup_{g\neq e \in G} gU$.

To show an open subgroup U is closed, we want to show that union of cosets gU, $g \notin U$ is open. As a union of open sets is open, it suffices to show that the cosets gU are open.

In a profinite group, we can see that $\forall g \in \varprojlim G_\alpha$ $f: (\varprojlim G_\alpha) \to (\varprojlim G_\alpha)$ such that $f(x) = gx$ is a homeomorphism.

Def: A function $f: X \to Y$ between two topological spaces is a homeomorphism if:

(1) f is a bijection
(2) f is continuous (preimages of open sets are open)
(3) f^{-1} is continuous (images of open sets are open)
In our case, $f^{-1}(x) = g^{-1}x$
f is a homeomorphism because (left) multiplication by g is continuous on the product of finite groups (with U a subgroup) and as the topology $\varprojlim G_\alpha$ is the induced topology, multiplication by g is continuous on $\varprojlim G_\alpha$ as well. The same can be said for multiplication by g^{-1}, so f (and f^{-1}) is a homeomorphism. This implies that U is homeomorphic to gU under this map, so all gU are open $\Rightarrow \bigcup_{\text{finite}} gU$ are open $\Rightarrow U^c$ is closed $\Rightarrow U$ is open. Therefore, open subgroups are closed.

(ii) Next, we have show open subgroups U have finite index. The index of U is the number of cosets gU, with $\varprojlim G_\alpha$ the disjoint union of cosets gU. As $\varprojlim G_\alpha$ is compact, it follows that the number of cosets is finite as any open cover can be reduced to a finite open cover, and we can take the cover given by open subsets gU, which are disjoint, to show that $\varprojlim G_\alpha$ must have a finite open cover. Therefore, U must have finite index as a disjoint open cover cannot be refined further.

(iii) Finally, we must show closed subgroups of finite index are open. Let V be a closed subgroup of finite index and consider its complement. It must be a disjoint and finite (because of the finite index assumption) union of cosets gV, $g \notin V$. As V is homeomorphic to gV, if gV is open, V must be open as well. Therefore, closed subgroups of finite index are open and open subgroups are closed subgroups of finite index. So in a profinite group, the open subgroups correspond exactly to the closed subgroups of finite index.

Remark: Not all subgroups of finite index in a profinite group are open (in general)

Remarks: (on previous theorem) We can extend this classification to say profinite groups are the topological groups which are compact and totally disconnected and Hausdorff (for $x, y \in X$: $\exists U, V \subset X$ disjoint such that $x \in U, y \in V$)

We can use this topology to construct an analogue of the Fundamental Theorem of Galois Theory for infinite extensions.

Main Thm: If L_i is a subextension of the Galois extension L/K, then $Gal(L/L_i)$ is a closed subgroup of $Gal(L/K)$. Moreover, for $H = Gal(L/L_i)$, $L_i = L^H$, there exists an inclusion-reversing bijection between the intermediate fields $L \subset L_i \subset K$ and the closed subgroups $H \subset Gal(L/K)$. A subextension L_i/K is Galois $\Leftrightarrow$ $Gal(L/L_i)$ is normal in $Gal(L/K)$ in this case there is a natural isomorphism $Gal(L_i/K) \cong Gal(L/K)/Gal(L/L_i)$

Remark: This is very similar to the Fundamental Theorem of Galois Theory in the finite case. The key difference is that we restrict the bijection to closed subgroups of $Gal(L/K)$ rather than all subgroups

(Thm): If E/F is a finite Galois extension with $Gal(E/F)$, then there exists an order-reversing bijection between intermediate subfields $E \supseteq L \supseteq F$ and subgroups H of G such that $L \mapsto Gal(E/L)$ and $E^H \mapsfrom H$ are inverses of each other

Remark: In our case, we have $L_i \longmapsto Gal(L/L_i) = H$
$L_i = L^H \longmapsfrom H$

Remark: There exist non-closed subgroups in the Galois group of any infinite extension.

Corollary: For L/K Galois Extension and H a subgroup of $Gal(L/K)$ Then the following are equivalent:

1. H is open in $Gal(L/K)$
2. H is closed in $Gal(L/K)$ and the fixed field L^H has finite index over K.