Infinite Galois Theory

Joshua Ruiter

October 8, 2019

Contents

These notes were written for a student algebra seminar talk given at MSU in January, 2018. The main sources are Milne [1] and Szamuely [2]. Thanks to Igor Rapinchuk for help refining the presentation/sequence of topics.

1 Galois theory

1.1 Review of field extension terminology

Definition 1.1. *A field extension Ω/F is **normal** if it is a splitting field of a family of polynomials in $F[x]$. (It is generated over F by roots of all polynomials in the family, and all the polynomials in the family factor linearly in Ω.)*

Definition 1.2. *A field extension Ω/F is **separable** if it is algebraic and if for every $\alpha \in \Omega$, the irreducible polynomial of α over F has no repeated roots.*

Definition 1.3. *A field extension Ω/F is **Galois** if it is normal and separable. If Ω/F is a Galois extension, the **Galois group**, denoted $\mathrm{Gal}(\Omega/F)$, is the group of automorphisms of Ω that fix F.*

Definition 1.4. *Let $G = \mathrm{Gal}(\Omega/F)$ and let $H \subset G$ be a subgroup. The **fixed field** of H, denoted Ω^H, is the set*

$$\Omega^H = \{x \in \Omega : \sigma x = x \ \forall \sigma \in H\}$$

(This is in fact a field.)

Proposition 1.1 (Milne Prop 7.3)**.** *Let Ω/F be Galois and $G = \mathrm{Gal}(\Omega/F)$. Let E be an intermediate field, $F \subset E \subset \Omega$. Then Ω/E is Galois, and $\mathrm{Gal}(\Omega/E)$ is a subgroup of G.*

Proof. Regardless of whether Ω/E is Galois, the automorphisms of Ω that fix E form a subgroup of G, so the second statement has nothing to prove. Recall that separable extensions form a distinguished class, and normal extensions remain normal under lifting. That is, if Ω/F is separable, then Ω/E and E/F are separable, and if Ω/F is normal, then Ω/E is normal. Thus Ω/E is normal and separable, so it is Galois. □

Note: For a tower $F \subset E \subset \Omega$, it is NOT true that E/F is necessarily Galois. Separable extension form a distinguished class, but normal extensions don't. So E/F is always separable, but it may not be normal.

Proposition 1.2 (Milne Prop 7.4)**.** *Let Ω/F be Galois, and let $F \subset E \subset \Omega$ be an intermediate field. Every F-linear map $E \to \Omega$ extends to an F-linear isomorphism $\Omega \to \Omega$.*

Proof. Requires Zorn's lemma, omitted. □

1.2 The Galois correspondence

Below is the finite Galois correspondence, followed immediately by the more general version. The differences are underlined for emphasis.

Theorem 1.3 (Fundamental Theorem of Finite Galois Theory)**.** *Let Ω be a $\underline{\text{finite}}$ Galois extension of a field F, and let $G = \mathrm{Gal}(\Omega/F)$. There is a bijection*

$$\begin{aligned} \{\textit{subgroups of } G\} &\longleftrightarrow \{\textit{intermediate fields } F \subset E \subset \Omega\} \\ H &\longmapsto \Omega^H \\ \mathrm{Gal}(\Omega/E) &\longleftarrow\!\shortmid E \end{aligned}$$

Notably, $\Omega^{\mathrm{Gal}(\Omega/E)} = E$. This bijection also has the following properties:

(i) The correspondence is inclusion reversing. That is, $H_1 \subset H_2 \iff \Omega^{H_1} \supset \Omega^{H_2}$.

(ii) Subgroup conjugation corresponds to left action. That is, $\Omega^{\sigma H \sigma^{-1}} = \sigma(\Omega^H)$ *and* $\sigma \operatorname{Gal}(\Omega/E)\sigma^{-1} = \operatorname{Gal}(\Omega/\sigma E)$. *More succintly, if* $H \leftrightarrow E$ *then* $\sigma H \sigma^{-1} \leftrightarrow \sigma E$.

(iii) A subgroup $H \subset G$ *is normal if and only if* Ω^H/F *is Galois. In this case,* $\operatorname{Gal}(\Omega^H/F) \cong G/H$.

(iv) If $H \subset G$ *is normal, then* $[G : H] = [\Omega^H : F]$. *(*$[G : H]$ *is the index of* H *in* G*, and* $[\Omega^H : F]$ *is the degree of the field extension.)*

Theorem 1.4 (Fundamental Theorem of Galois Theory)**.** *Let* Ω *be a Galois extension of a field* F*, and let* $G = \operatorname{Gal}(\Omega/F)$. *There is a bijection*

$$\begin{aligned} \{\underline{\textit{closed}} \textit{ subgroups of } G\} &\longleftrightarrow \{\textit{intermediate fields } F \subset E \subset \Omega\} \\ H &\longmapsto \Omega^H \\ \operatorname{Gal}(\Omega/E) &\longleftarrow\!\shortmid\, E \end{aligned}$$

Notably, $\Omega^{\operatorname{Gal}(\Omega/E)} = E$. *This bijection also has the following properties:*

(i) The correspondence is inclusion reversing. That is, $H_1 \subset H_2 \iff \Omega^{H_1} \supset \Omega^{H_2}$.

(ii) Subgroup conjugation corresponds to left action. That is, $\Omega^{\sigma H \sigma^{-1}} = \sigma(\Omega^H)$ *and* $\sigma \operatorname{Gal}(\Omega/E)\sigma^{-1} = \operatorname{Gal}(\Omega/\sigma E)$. *More succintly, if* $H \leftrightarrow E$ *then* $\sigma H \sigma^{-1} \leftrightarrow \sigma E$.

(iii) A closed subgroup $H \subset G$ *is normal if and only if* Ω^H/F *is Galois. In this case,* $\operatorname{Gal}(\Omega^H/F) \cong G/H$.

(iv) A closed subgroup $H \subset G$ *is open if and only if* Ω^H/F *is a finite extension. In this case,* $[G : H] = [\Omega^H : F]$. *(*$[G : H]$ *is the index of* H *in* G*, and* $[\Omega^H : F]$ *is the degree of the field extension.)*

Assume for the moment that we only know the theorem holds in the finite case. We would like to understand what happens when Ω/F is an infinite extension. Is the exact same theorem still true? Most of the results leading up to this don't care about the degree of the extension. However, some do require a finite extension, so this theorem as stated (without "closed") is false if Ω/F is infinite. Dedekind was the first to give examples of a subgroup that doesn't correspond to a subextension.

Lemma 1.5. *An extension* Ω/F *is Galois if and only if it is a union of finite Galois extensions.*

Proof. If Ω is a union of finite Galois extensions, then it is the compositum of those extensions. The compositum of Galois extensions is Galois (because normal and separable extensions have these properties), so Ω/F is Galois.

Suppose Ω/F is Galois and let E be an intermediate field, which is finite Galois over F. Since E/F is separable, by the Primitive Element Theorem it has the form $E = F(\alpha)$ for some $\alpha \in \Omega$. Let f be the irreducible/minimal polynomial of α over F. Then E embeds into the splitting field of f, which is finite Galois over F. Then Ω is the union of all of these, since each $\alpha \in \Omega$ is contained in some such intermediate field. □

This lemma suggests that we might be able to understand an infinite Galois extension just by piecing together all the finite Galois subextensions in the right way. If we have a tower $F \subset E_1 \subset E_2 \subset E_3 \subset \Omega$ where E_i are all finite Galois extensions of F, we have restriction homomorphisms in the following commutative diagram.

$$\begin{tikzcd}
\mathrm{Gal}(\Omega/F) \arrow[r] & \ldots \arrow[r] & \mathrm{Gal}(E_3/F) \arrow[r, "\phi_2^3"] \arrow[rr, bend right, "\phi_1^3"'] & \mathrm{Gal}(E_2/F) \arrow[r, "\phi_1^2"] & \mathrm{Gal}(E/F)
\end{tikzcd}$$

where $\phi_i^j(\sigma) = \sigma|_{E_i}$. If we have a longer chain, $F \subset E_1 \subset E_2 \subset \ldots \subset \Omega$, we can extend this diagram to the left forever. This suggests that if we take some sort of limit, we can approximate $\mathrm{Gal}(\Omega/F)$. We're going to do this with inverse limits.

2 Inverse limits

2.1 Definitions

Definition 2.1. *A* ***directed set*** *is a partially ordered set $(I, \leq)$ such that for all $i, j \in I$, there exists $k \in I$ so that $i \leq k$ and $j \leq k$.*

Definition 2.2. *Let $\mathcal{C}$ be a category and $(I, \leq)$ a directed set. An* ***inverse system*** *in $\mathcal{C}$ is a family $(A_i)_{i \in I}$ of objects together with a family $(p_i^j : A_j \to A_i)_{i \leq j}$ of morphisms such that $p_i^i = \mathrm{Id}_{A_i}$ and $p_i^j \circ p_j^k = p_i^k$ for all $i \leq j \leq k$.*

$$\begin{tikzcd}
& A_k \arrow[dl, "p_j^k"'] \arrow[dr, "p_i^k"] & \\
A_j \arrow[rr, "p_i^j"'] & & A_i
\end{tikzcd}$$

Definition 2.3. *Let $(A_i), (p_i^j)$ be an inverse system. An* ***inverse limit*** *of this system is an object A along with a family of morphisms $p_j : A \to A_j$ satisfying $p_i^j \circ p_j = p_i$ for all $i \leq j$,*

$$\begin{tikzcd}
& A \arrow[dl, "p_j"'] \arrow[dr, "p_i"] & \\
A_j \arrow[rr, "p_i^j"'] & & A_i
\end{tikzcd}$$

as well as the following universal property. For any object B and family of morphisms $q_j : B \to A_j$ satisfying $p_i^j \circ q_j = q_i$ for $i \leq j$, there exists a unique morphism $r : B \to A$ such that $p_j \circ r = q_j$ for all j.

$$\begin{tikzcd}
& B \arrow[d, dotted, "r"] \arrow[ddl, bend right, "q_j"'] \arrow[ddr, bend left, "q_i"] & \\
& A \arrow[dl, "p_j"] \arrow[dr, "p_i"'] & \\
A_j \arrow[rr, "p_i^j"'] & & A_i
\end{tikzcd}$$

Definition 2.4. *Let $(G_i, p_i^j : G_j \to G_i)$ be an inverse system of groups. The* ***inverse limit*** *of this system, denoted $\varprojlim G_i$, is*

$$\varprojlim G_i = \left\{ (g_i) \in \prod_i G_i : p_i^j(g_j) = g_i,\ \forall i \leq j \right\}$$

One can check that this is a subgroup of the product $\prod G_i$. One needs to check that the universal property holds; see the next lemma.

In just a minute, we'll see an example of a direct limit arising from an infinite Galois extension.

Lemma 2.1. *The group defined above satisfies the universal property of inverse limits.*

Proof. Let (H, q_i) be a family with $q_i : H \to G_i$ satisfying $p_i^j \circ q_j = q_i$. Then the homomorphism

$$H \to \prod_i G_i \qquad h \mapsto (q_i(h))$$

has image contained in $\varprojlim G_i$, because $p_i^j(q_j(h)) = q_i(h)$. It is also the unique morphism $H \to G$ mapping q_i to p_i, so this is the required morphism for the universal property. □

Definition 2.5. *A* ***profinite*** *group is any group that is an inverse limit of finite groups.*

2.2 Galois groups as inverse limits

Let Ω/F be a Galois extension. Let I be the set of intermediate fields $F \subset E \subset \Omega$ such that E/F is finite Galois. I is partially ordered by inclusion and forms a directed set, since any two E, E' are contained in the compositum EE' (compositum taken in Ω).

For each $E \in I$, we have the finite group $\mathrm{Gal}(E/F)$, and for $E \subset E'$ we have a restriction homomorphism $p_E^{E'} : \mathrm{Gal}(E'/F) \to \mathrm{Gal}(E/F), \sigma \mapsto \sigma|_E$, so we get an inverse system of finite groups, so we can take the inverse limit.

Proposition 2.2. *Let Ω/F be a Galois extension. Then*

$$\begin{gathered} \mathrm{Gal}(\Omega/F) \to \varprojlim \mathrm{Gal}(E/F) \\ \sigma \mapsto (\sigma|_E) \end{gathered}$$

is a group isomorphism.

Proof. We check that it actually maps into $\varprojlim \mathrm{Gal}(E/F)$. We need to check that $p_E^{E'}(\sigma|_{E'}) = \sigma|_E$, but this is true by definition of $p_E^{E'}$. It is a group homomorphism because $\sigma\tau \mapsto ((\sigma\tau)|_E) = (\sigma|_E \tau|_E) = (\sigma|_E)(\tau|_E)$ for any $\sigma, \tau \in \mathrm{Gal}(\Omega/F)$. The kernel is

$$\ker = \{\sigma \in \mathrm{Gal}(\Omega/F) : \sigma|_E = \mathrm{Id}_E\}$$

Since $\Omega = \bigcup E$, anything in the kernel is the identity on all of Ω. Thus the kernel is trivial so the map is injective.

Finally, suppose (σ_E) is in $\varprojlim \mathrm{Gal}(E/F)$, with $\sigma_E \in \mathrm{Gal}(E/F)$. Then we define $\sigma : \Omega \to \Omega$ by $\sigma(x) = \sigma_E(x)$ for $x \in E$. As already noted, $\Omega = \bigcup E$, so this defines σ on all of Ω. We need to check that this is well-defined, so we need to check that if $x \in E \cap E'$, then $\sigma_E(x) = \sigma_{E'}(x)$. Note that $E \cap E'$ is also a finite Galois extension of F. (Intersection of normal extensions is normal.)

$$\begin{tikzcd}
 & \Omega \arrow[dl, dash] \arrow[dr, dash] & \\
E \arrow[dr, dash] & & E' \arrow[dl, dash] \\
 & E \cap E' \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

Since $(\sigma_E) \in \varprojlim \mathrm{Gal}(E/F)$,

$$p^E_{E\cap E'}(\sigma_E) = \sigma_{E\cap E'} \qquad p^{E'}_{E\cap E'}(\sigma_{E'}) = \sigma_{E\cap E'}$$

thus σ_E and $\sigma_{E'}$ agree on $E \cap E'$, which contains x, so σ is well-defined. By construction, $\sigma|_E = \sigma_E$, so our map is surjective. □

Corollary 2.3 (Milne 7.6)**.** *Let Ω/F be a Galois extension, and $F \subset E \subset \Omega$ be an intermediate field, with E/F finite Galois. Then the map*

$$\mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F) \qquad \sigma \mapsto \sigma|_E$$

is a continuous surjection, if we put the discrete topology on $\mathrm{Gal}(E/F)$*.*

Proof. If $\sigma_E \in \mathrm{Gal}(E/F)$, and view it as an F-linear map $E \to \Omega$. By Proposition 1.2, σ_E extends to an F-linear isomorphism $\sigma : \Omega \to \Omega$, which means precisely that $\sigma|_E = \sigma_E$. Hence the map is surjective. It is continuous because it is the canonical map associated with the direct limit. □

2.3 Example - absolute Galois group of a finite field

Definition 2.6. *Let F be a field, and F^{sep} the separable closure (maximal Galois extension of F). The **absolute Galois group** of F is $\mathrm{Gal}(F^{\mathrm{sep}}/F)$.*

Now we use the results we developed to compute the absolute Galois group of a finite field with p elements. Let p be a prime and let $\mathbb{F}_p$ be the finite field with p elements. Let Ω be an algebraic closure of $\mathbb{F}_p$, so $\Omega/\mathbb{F}_p$ is Galois (since $\mathbb{F}_p$ is a perfect field).

Using our direct limit characterization, we can can get a handle on the structure of $\mathrm{Gal}(\Omega/\mathbb{F}_p)$. We know that the finite Galois subextensions $\mathbb{F}_p \subset E \subset \Omega$ are exactly the finite fields $\mathbb{F}_{p^n}$ for $n \in \mathbb{Z}^+$, and $\mathbb{F}_{p^m}$ is contained in $\mathbb{F}_{p^n}$ if and only if $m|n$, so that's our partial ordering.

$$\mathbb{F}_p \ \subset\ \mathbb{F}_{p^n} \ \subset\ \dots \ \subset\ \Omega$$

Furthermore, we know exactly what these finite Galois groups are. The Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n, generated by the Frobenius automorphism $x \mapsto x^p$. For $m|n$, the restriction map

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \to \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$$

sends σ (Frobenius) to itself, so this is just the map

$$\phi^n_m : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \qquad x \mapsto x \bmod m$$

The inverse limit of this system is called $\widehat{\mathbb{Z}}$. This looks like

$$\widehat{\mathbb{Z}} = \left\{ (a_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z} : \phi^n_m(a_n) = a_m, \ \forall m|n \right\}$$

Notice that the condition $\phi^n_m(a_n) = a_m$ is equivalent to $a_n \bmod m = a_m$ which is equivalent to $a_n \equiv a_m \bmod m$.

What are some example elements in $\widehat{\mathbb{Z}}$? The "constant sequences" such as $(\overline{1}, \overline{1}, \overline{1}, \ldots), (\overline{2}, \overline{2}, \overline{2}, \ldots)$ (these actually form an embedded copy of $\mathbb{Z}$ in $\widetilde{\mathbb{Z}}$). Here's a family of elements not of this form. Choose a prime p, and let $a_n = \overline{1}$ if n is a power of p and $a_n = \overline{0}$ else. For $p = 2$, this looks like

$$(a_n) = (\overline{0}, \overline{1}, \overline{0}, \overline{1}, \overline{0}, \overline{0}, \overline{0}, \overline{1}, \overline{0} \ldots)$$

(Remember that $\overline{1} = \overline{0}$ in $\mathbb{Z}/1\mathbb{Z}$, so it doesn't really matter how we write a_1.)

Note: For those who are interested, $\widehat{\mathbb{Z}}$ is closely related to the p-adic integers. It is isomorphic the product over all $\mathbb{Z}_p$.

2.4 The Krull topology

Definition 2.7. *A* ***topological group*** *is a topological space with a group structure such that the multiplication map $G \times G \to G, (x, y) \mapsto xy$ and the inversion map $G \to G, x \mapsto x^{-1}$ are continuous. ($G \times G$ has the product topology.)*

If we have an inverse system of topological groups, the inverse limit in the category of groups is also an inverse limit in the category of topological groups, provided $\varprojlim G_i$ has the subspace topology from the product topology on $\prod G_i$. We just need to observe that the projection maps are continuous, so everything is still a morphism.

Any profinite group has a "natural" topology. We endow the finite groups in the system with the discrete topology, then give $\prod G_i$ the product topology, then give $\varprojlim G_i$ the subspace topology from this. This makes $\varprojlim G_i$ a topological group.

So we have a topology on the inverse limit of Galois groups above. Then using our isomorphism from Proposition 2.2, there is a unique topology on $\mathrm{Gal}(\Omega/F)$ making this group isomorphism into a homeomorphism as well. This topology is called the **Krull topology** on $\mathrm{Gal}(\Omega/F)$.

Now that we have defined this topology, what can we say about it? What does a typical open set look like? We know that the projection maps $p_i : G \to G_i$ are continuous, so the preimage of any $x \in G_i$ is an open subset of G, since G_i is discrete. In particular, the preimage of the identity of G_i is open.

Lemma 2.4. *Let* (G_i, p_i^j) *be an inverse system of finite groups, and let* $G = \varprojlim G_i$. *The kernels* $\ker p_i$ *are a family of open neighborhoods of the identity in* G, *consisting of normal subgroups of finite index.*

Proof. G_i is discrete, so the identity $\{e_i\}$ is open. The projection $p_i : G \to G_i$ is continuous, so the preimage $\ker p_i$ is open. Kernels are always normal subgroups, so it contains the identity. It has finite index because $G/\ker p_i \cong G_i$, and G_i is finite. □

We can actually say more than the previous lemma - the kernels form a neighborhood base of the identity in G, but we won't go into the definition of a neighborhood base.

Proposition 2.5. *Let* $(G_i, p_i^j : G_j \to G_i)$ *be an inversely directed system of finite groups, and give each the discrete topology. Then* $\varprojlim G_i$ *is Hausdorff, compact, and totally disconnected.*

Proof. Let $G = \varprojlim G_i$. Subspaces and products of Hausdorff spaces are Hausdorff, so $\prod G_i$ is Hausdorff, so the subspace G is Hausdorff. Similarly, subspaces and products of totally disconnected spaces are totally disconnected, so G is totally disconnected.

Now we want to show compactness. Each G_i is compact, so by Tychonoff's Theorem $\prod G_i$ is compact. Thus it is sufficient to show that G is closed in $\prod G_i$, since closed subspaces of compact spaces are compact. Choose $(x_i) \in (\prod G_i) \setminus G$. Then there exist j, k so that $p_j^k(x_k) \neq x_j$. The set

$$\{(g_i) : g_j = x_j, g_k = x_k\}$$

is open in $\prod G_i$ and lies entirely in the complement of G, so the complement of G is open, so G is closed. □

Note: The converse to the above is also true, that any topological group with those properties is profinite. That direction is much harder to prove.

Corollary 2.6. *For any Galois extension* Ω/F, $\mathrm{Gal}(\Omega/F)$ *is Hausdorff, compact, and totally disconnected.*

Proof. Immediate consequence of Propositions 2.2 and 2.5. □

3 The Galois correspondence again

We can now update our statement of the Galois correspondence to include infinite extensions. We haven't actually proved it, but at least now we know what topology is behind the phrase "closed subgroup." This phrase is the key difference in passing to infinite Galois extensions - we no longer have a correspondence with all subgroups, just the closed ones. Let's prove some of it at least.

Lemma 3.1. *Let* G *be a topological group.*

I. *Every open subgroup of* G *is closed.*

II. *Every closed subgroup of finite index is open.*

Proof. (I) Let H be an open subgroup. For any $g \in G$, the map $G \to G, x \mapsto gx$ is a topological group isomorphism. In particular, the cosets gH are all homeomorphic to H, so they are open. Since $G = \bigsqcup gH$, the complement of H is a union of open sets, so it is open, so H is closed. This proves the first statement.

(II) Let H be a closed subgroup of finite index. As before, $G = \bigsqcup gH$, but now with each gH closed. Since H has finite index, the complement of H is a finite union of closed subsets, so it is closed, so H is open. □

Definition 3.1. *Let $G = \mathrm{Gal}(\Omega/F)$ and let $S \subset \Omega$ be a finite set. Define*

$$G(S) = \{\sigma \in G : \sigma s = s,\ \forall s \in S\}$$

This is the stabilizer of S in the action of G on Ω. Note that $G(S) = \mathrm{Aut}(\Omega/F(S))$, where $F(S)$ is the extension of F generated by S.

Definition 3.2. *Let Ω/F be a Galois extension. A subset $S \subset \Omega$ is* ***stable under*** *G if for $\sigma \in G$, $\sigma(S) \subset S$.*

Lemma 3.2. *Let Ω/F be a Galois extension, and let $S \subset \Omega$ be a finite set stable under G. Then we have a short exact sequence of groups*

$$1 \to G(S) \to \mathrm{Gal}(\Omega/F) \xrightarrow{\pi} \mathrm{Gal}(F(S)/F) \to 1$$

Hence $G(S)$ is an open normal subgroup of G of finite index.

Proof. First, note that for such S, $F(S)/F$ is Galois. We know it is separable, we just need to check that it is normal. For $\alpha \in S$, let f_α be the irreducible/minimal polynomial of α over F. Since S is stable under G, all roots of f_α are in S. Thus $F(S)$ is the splitting field of the family f_α, so this is a normal (and hence Galois) extension.

If $\sigma \in \ker \pi$, then $\sigma|_{F(S)} = \mathrm{Id}$, so $\sigma|_S = \mathrm{Id}$ and $\sigma \in G(S)$. For the reverse inclusion, if $\sigma \in G(S)$, then $\sigma|_F = \mathrm{Id}$ and $\sigma|_S = \mathrm{Id}$, and since $F(S)$ is generated by S over F, $\sigma|_{F(S)} = \mathrm{Id}$, so $\sigma \in \ker \pi$. Hence $\ker \pi = G(S)$.By Corollary 2.3, π is conintuous and surjective, so the sequence is exact as claimed. Since π is continuous and $\mathrm{Gal}(F(S)/F)$ is discrete, the kernel $G(S)$ is a open normal subgroup. □

Lemma 3.3. *Let Ω/F be a Galois extension and $G = \mathrm{Gal}(\Omega/F)$, and let $S \subset \Omega$ be any finite subset. Then $G(S)$ is an open subgroup of G of finite index. It is normal if and only if S is stable under G.*

Proof. That $G(S)$ is a subgroup of finite index is clear, what is not so clear is that it is a open and normal. From the previous lemma, we know this is true in the case where S is stable under G. Let

$$\overline{S} = \{\tau s : \tau \in G\}$$

be the set of all Galois conjugates of S, so $\overline{S}$ is stable under G. It is clear that $G(\overline{S}) \subset G(S)$, so $G(\overline{S})$ is an open normal subgroup of finite index. We claim that

$$G(S) = \bigcup_{\sigma \in G(S)} \sigma G(\overline{S})$$

The inclusion $\subset$ is obvious, since $\sigma \in \sigma G(\overline{S})$. The reverse inclusion is also obvious, since for $\sigma \in G(S)$ and $\tau \in G(\overline{S})$, $\sigma\tau$ fixes S, so $\sigma G(\overline{S}) \subset G(S)$. Since each $G(\overline{S})$ is open and left multiplication by σ is a homeomorphism, $\sigma G(\overline{S})$ is also open, so the union above is open.

Regarding the statement about normality, we already know that if S is stable under G, $G(S) = G(\overline{S})$ is normal. For the converse, notice that for $\tau \in G$, we have

$$\begin{aligned} \tau G(S)\tau^{-1} &= \left\{\tau\sigma\tau^{-1} : \sigma s = s, \forall s \in S\right\} \\ &= \left\{\beta : \tau^{-1}\beta\tau s = s, \forall s \in S\right\} \\ &= \{\beta : \beta\tau s = \tau s, \forall s \in S\} \\ &= G(\tau S) \end{aligned}$$

If S is stable under G, then $\tau S = S$ hence $\tau G(S)\tau^{-1} = G(S)$ for all $\tau \in G$, which is precisely the condition that $G(S)$ is normal. □

Proposition 3.4. *Let $G = \mathrm{Gal}(\Omega/F)$, and let E an intermediate field, $F \subset E \subset \Omega$. Then $\mathrm{Gal}(\Omega/E)$ is closed in G.*

Proof. For each finite subset $S \subset E$, $G(S)$ is an open subgroup of G by Lemma 3.3, so it also closed by Lemma 3.1. We claim that

$$\mathrm{Gal}(\Omega/E) = \bigcap_{S\subset E,\text{ finite}} G(S)$$

One inclusion is easy: $\mathrm{Gal}(\Omega/E)$ is contained in each $G(S)$, since elements of $\mathrm{Gal}(\Omega/E)$ fix every element of E. For the reverse inclusion, it is clear that each $\alpha \in E$ is contained in some S, so if σ fixes each S, it fixes E. Since we have written $\mathrm{Gal}(\Omega/E)$ as an intersection of closed sets, it is closed. □

We know that if we take any subgroup of $\mathrm{Gal}(\Omega/F)$, we can take its fixed field and get an intermediate field, with associated Galois group $\mathrm{Gal}(\Omega/\Omega^H)$. Suppose H is not closed. Then the subgroup corresponding to this intermediate field can't be H, so what is it? The next proposition answers this question.

Proposition 3.5. *Let $G = \mathrm{Gal}(\Omega/F)$, and let $H \subset G$ be a subgroup. Then $\mathrm{Gal}(\Omega/\Omega^H)$ is the closure of H.*

Proof. I don't understand this proof well enough to give a succinct proof appropriate for a seminar. □

A natural question to ask is, "Are all subgroups of the Galois group closed?" If this is the case, then the restriction is not actually a restriction, just a vacuous condition. However, there are subgroups that are not closed. Dedekind was the first person to find non-closed subgroups in specific cases. Krull later showed that ANY infinite Galois extension includes non-closed subgroups. Thus, the restriction to closed subgroups is highly nontrivial.

3.1 Example - Galois group of infinite cyclotomic extension of $\mathbb{Q}$

In this section, we describe the infinite Galois group of the infinite extension $\Omega/\mathbb{Q}$, where Ω is formed by adjoining all roots of unity to $\mathbb{Q}$.

Definition 3.3. *A field extension E/F is* **cyclotomic** *if E is the splitting field of $x^n - 1$ over F for some n.*

Proposition 3.6. *Let E_n be the splitting field of $x^n - 1$ over $\mathbb{Q}$. Then* $\mathrm{Gal}(E_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. We don't have time or space to prove this here. □

All E_n are contained in $\overline{\mathbb{Q}}$, so we can take the compositum over all n; we will denote this compositum by Ω.

$$\Omega = E_1 E_2 E_3 \dots$$

Since the compositum of normal extensions is normal, $\Omega/\mathbb{Q}$ is normal, and since $\mathrm{char}\,\mathbb{Q} = 0$, all extensions of $\mathbb{Q}$ are separable, so $\Omega/\mathbb{Q}$ is Galois. Next we wanto to take the inverse limit over Galois groups of finite Galois subextensions. While not every finite Galois subextension here is one of the E_n, we do have the following.

Theorem 3.7 (Kronecker-Weber)**.** *Every finite abelian Galois extension of $\mathbb{Q}$ is contained in some E_n.*

Because of this, when forming the direct limit over all finite Galois subextensions, it's sufficient to just consider the E_n extensions. I don't understand how to make this precise, but it's something I've been told.

Thus, the inverse system we should consider is the groups $(\mathbb{Z}/n\mathbb{Z})^\times$ for $n \geq 1$, partially ordered by divisibility $(m|n)$. When $m|n$, $E_m \subset E_n$, so we get a restriction homomorphism $\mathrm{Gal}(E_n/\mathbb{Q}) \to \mathrm{Gal}(E_m\mathbb{Q})$ which is given by

$$\begin{aligned} \mathrm{Gal}(E_n/\mathbb{Q}) &\to \mathrm{Gal}(E_m/\mathbb{Q}) \\ (\mathbb{Z}/n\mathbb{Z})^\times &\to (\mathbb{Z}/m\mathbb{Z})^\times \\ x &\mapsto x \bmod m \end{aligned}$$

And by our theorem, $\mathrm{Gal}(\Omega/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times$.

$$\varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = \left\{ (a_n) \in \prod_{n=1}^{\infty} (\mathbb{Z}/n\mathbb{Z})^\times : a_n \equiv a_m \bmod m,\ \forall m|n \right\}$$

If we put a ring structure on $\widehat{\mathbb{Z}}$ (induced by mulitplication in each $\mathbb{Z}/n\mathbb{Z}$), then one can show that this inverse limit above is the group of units of $\widehat{\mathbb{Z}}$.

References

[1] James S. Milne. Fields and galois theory (v4.30), 2012. Available at www.jmilne.org/math/.

[2] Tamás Szamuley. Galois groups and fundamental groups, 2009.