INFINITE GALOIS THEORY

Yassine El Maazouz

Contents

1. Preliminaries

Let k be a field and let us once and for all fix an algebraic closure $\overline{k}$. Let k^s be the separable closure of k in $\overline{k}$. The extension k^s/k comes with a Galois group $G := \mathrm{Gal}(k^s/k)$ which is called the absolute Galois group of k. The extension k^s/k has infinite degree and it contains all separable finite extensions of k. While the main theorem of Galois theory is stated for finite separable extensions of k, the same result does work well with infinite extensions. The following is a typical example of what can go wrong.

Example 1.1. — Assume $k = \mathbb{F}_p$ is the finite field with p-elements where p is a prime number. The algebraic closure $\overline{\mathbb{F}}_p$ is separable and its Galois group $G = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ contains a distinguished element of this Galois group which is the Frobenius morphism $\varphi : x \mapsto x^p$. For any finite extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is generated by the restriction $\varphi_n = \varphi_{|\mathbb{F}_{p^n}}$, so in other words $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \varphi_{|\mathbb{F}_{p^n}} \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Hence we get $G = \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ which is the arithmetic completion of $\mathbb{Z}$. However, the Frobenius automorphism does not generate the absolute Galois group, i.e. we do not have $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \langle \varphi \rangle$. To see that, let's consider an element $\sigma \in G$ and let's call σ_n its restriction to $\mathbb{F}_{p^n}$. We know that for each $n \geq 1$ there exists $a_n \in \mathbb{Z}$ such that $\sigma_n = \varphi_n^{a_n}$. These integers a_n have to satisfy the following condition for any integers $m|n$:

$$a_n = a_m \mod m.$$

Since we are looking for an element σ such that $\sigma \notin \langle \varphi \rangle$, it suffices to find such a sequence of integers that satisfy the additional condition that there exists no $a \in \mathbb{Z}$ such that $a_n = a \mod n$. Such a sequence of integers can be found as follows:

For every $n \geq 1$, write $n = p^{v_p(n)} n'$ where p does not divide n'. By Bezout's theorem exist $u_n, v_n \in \mathbb{Z}$ such that $u_n n' + v_n p^{v_p(n)} = 1$. The reader can check that picking $a_n = n' u_n$ solves the problem and we can thus find elements in G that are not powers of the Frobenius φ.

Also, when the extension is infinite, we no longer have the usual Galois correspondence between field extensions of k and subgroups of G. However we can mend this problem by changing the statement a little as we explain in the following sections.

2. A topology on the Galois group

To fix the statement of the Galois correspondence in the infinite extension case, we need to equip our group G with a what is called the *Krull topology*. Let K/k be a Galois extension of k and $\sigma \in G$ and lets consider the coset $\sigma \operatorname{Gal}(k^s/K)$. An element τ is in this coest if and only if $\sigma^{-1}\tau$ is trivial on K. So the bigger the extension K, the closer τ gets to σ. From this intuitive idea, we define a topology on G where the collection

$$\mathcal{B}_\sigma := \{\sigma \operatorname{Gal}(k^s/K), \text{ is a Galois extension of } k\}$$

is a basis of neighborhoods of the $\sigma \in G$.

Definition 2.1. — The *Krull topology* is the topology on G generated by the collections of open sets $\mathcal{B}_\sigma$ where $\sigma \in G$.

This topology makes G into a topological group as the following proposition explains.

Proposition 2.2. — *Equipped with the Krull topology, the Galois group G is a compact Hausdorff topological group.*

Proof. 1. First we show that the inverse map is continuous. Let $U \subset G$ be an open set in G and $H := \{\tau \in G, \tau^{-1} \in U\}$. For $\tau \in H$ we have $t^{-1} \in U$ so there exists a finite Galois extension K of k such that $\tau^{-1} \operatorname{Gal}(k^s/K) \subset U$. So by taking the inverse $\operatorname{Gal}(k^s/K)\tau \in H$. Hence $\tau(\tau^{-1} \operatorname{Gal}(k^s/K)\tau) \subset U$. Since K is a Galois extension, the group $\operatorname{Gal}(k^s/K)$ is normal so we have $(\tau^{-1} \operatorname{Gal}(k^s/K)\tau) = \operatorname{Gal}(k^s/K)$. Hence $\tau \operatorname{Gal}(k^s/K) \subset H$. So H is an open set and thus the inverse map is continuous.

2. Next, we show that the multiplication is continuous. Let U be an open set of G and $V = \{(\sigma, \tau), \sigma\tau \in U\}$ and $(\sigma, \tau) \in V$. Since U is an open set and $\sigma\tau \in U$ there exists a finite Galois extension K such that $\sigma\tau \operatorname{Gal}(k^s/K) \subset U$. Then, using the fact that $\operatorname{Gal}(k^s/K)$ is normal, we can see that $\sigma \operatorname{Gal}(k^s/K) \times \tau \operatorname{Gal}(k^s/K) \subset V$. So V is an open set in $G \times G$ and thus the multiplication map is continuous. So G is indeed a topological group.

3. Next we show that G is Hausdorff. If $\sigma \neq \tau \in G$, there exists a finite Galois extension K such that $\sigma_{|K} \neq \tau_{|K}$. So the two open sets $\sigma \operatorname{Gal}(k^s/K)$ and $\tau \operatorname{Gal}(k^s/K)$ are disjoint neighborhoods of σ and τ.

4. Finally, we get to the hard task which amounts to showing that G is compact. For this we consider the finite Galois groups $\operatorname{Gal}(K/k)$ where K ranges over all finite Galois extensions of k. These groups, endowed with the discrete topology, are compact. Their product is then compact by Tykhonov's theorem. The absolute Galois group $G =$

$\mathrm{Gal}(k^s/k)$, is the projective limit $\varprojlim_{K \text{ finite Galois}} \mathrm{Gal}(K/k)$ inside the product $\prod_{K \text{ finite Galois}} \mathrm{Gal}(K/k)$ and we have an injective homomorphism

$$\begin{aligned} \Phi : G &\to \prod_{K \text{ finite Galois}} \mathrm{Gal}(K/k) \\ \sigma &\mapsto (\sigma_{|K}). \end{aligned}$$

Our goal is to show that Φ is continuous, open (onto its image) and that its image $\Phi(G)$ is closed. Let $\sigma \in G$ and L a finite Galois extension of k and consider the set $U_{\sigma,L} := \{\sigma_{|L}\} \times \prod_{K \neq L} \mathrm{Gal}(K/k)$. The sets $U_{\sigma,L}$ form a basis of the product topology on $\prod_{K \text{ finite Galois}} \mathrm{Gal}(K/k)$. The preimage $\Phi^{-1}(U_{\sigma,L}) = \sigma \, \mathrm{Gal}(k^s/L)$ is an open set, so Φ is continuous. Also, we have $\Phi(\sigma \, \mathrm{Gal}(k^s/L)) = \Phi(G) \cap U_{\sigma,L}$. So the map $\Phi : G \to \Phi(G)$ is open for the induced topology on $\Phi(G)$. So Φ is a homeomorphism from G to its image. Finally to see that $\Phi(G)$ is closed in the space $\prod_{K \text{ finite Galois}} \mathrm{Gal}(K/k)$, we consider sets $V_{L/K}$ defined by

$$V_{L/K} := \left\{ (\sigma_F) \in \prod_F \mathrm{Gal}(F/k), (\sigma_L)_{|K} = \sigma_K \right\}.$$

We have $\Phi(G) = \varprojlim_{K \text{ finite Galois}} \mathrm{Gal}(K/k) = \bigcap_{K \subset L} V_{L/K}$. Then it suffices to show that the set $V_{L/K}$ is closed. To see why $V_{L/K}$ is closed, we write $\mathrm{Gal}(K/k) = \{\sigma_1, \ldots, \sigma_n\}$ and consider the sets $\Gamma_i \subset \mathrm{Gal}(L/k)$ defined as

$$\Gamma_i := \{\sigma \in \mathrm{Gal}(L/k), \sigma_{|K} = \sigma_i\}.$$

One can then check that

$$V_{L/K} := \bigcup_{i=1}^{n} \left(\{\sigma_i\} \times \Gamma_i \prod_{F \neq K, F \neq L} \mathrm{Gal}(F/k) \right).$$

So $V_{L/K}$ is a finite union of closed sets and hence is closed. We then deduce that $\Phi(G)$ is closed and sits insite the compact group $\prod_{K \text{ finite Galois}} \mathrm{Gal}(K/k)$, so $\Phi(G)$ is compact. Now, since $\Phi : G \to \Phi(G)$ is a homeomorphism we deduce that G is compact.

□

Remark 2.3. — Notice that the previous result is valid, not just for the separable closure k^s, but for any separable extensions F of k.

3. The Galois correspondence

Now that we have equipped Galois groups with a nice topology, we are ready to state the general Galois correspondence.

Theorem 3.1. — *Let F be a separable extension of k. The map $K \mapsto \mathrm{Gal}(F/K)$ is a bijection between subextensions K of k inside F and closed subgroups of $\mathrm{Gal}(F/k)$. Moreover, the open subgroups of $\mathrm{Gal}(F/k)$ correspond exactly to the finite extensions K/k.*

Proof. First notice that any open subgroup H of $\mathrm{Gal}(F/k)$ is also closed. This is a general fact for topological groups. To see why we write $\mathrm{Gal}(F/k) \setminus H = \bigcup_{\sigma \notin H} \sigma H$. So The complement of H is open as a union of open sets. Hence H is also closed. Now if K/k is a finite subextension then $\mathrm{Gal}(F/K)$ is open because any $\sigma \in \mathrm{Gal}(F/K)$ has a neighborhood $\sigma \,\mathrm{Gal}(F/K^{nor})$ where K^{nor} is the Galois closure of K in F. So for any finite subextension K the group $\mathrm{Gal}(F/K)$ is open and hence also closed. If K is an general extension then

$$\mathrm{Gal}(F/K) = \bigcap_{K_i/k \text{ finite}} \mathrm{Gal}(F/K),$$

so $\mathrm{Gal}(F/K)$ is a closed subgroup. Hence the map $K \mapsto \mathrm{Gal}(F/K)$ taking subextension to closed subgroups is indeed well defined. Moreover, this map is injective since K is the fixed exactly the subfield of F fixed by $\mathrm{Gal}(F/K)$. It now remains to show surjectivity. To see why this map is surjective, fix a closed subgroup H of $\mathrm{Gal}(F/k)$. We need to show that $H = \mathrm{Gal}(F/K)$ where $K = F^H$ is the field fixed by H. The inclusion $H \subset \mathrm{Gal}(F/K)$ is fairly clear. Now, if $\sigma \in \mathrm{Gal}(F/K)$ and L/K a finite Galois subextension of F/K, then $\sigma \,\mathrm{Gal}(F/L)$ is an open neighborhood of σ in $\mathrm{Gal}(F/K)$. The restriction map $H \to \mathrm{Gal}(L/K)$ sending τ to $\tau_{|L}$ is surjective. To see why, consider $H_{|L}$ the image of H under restriction to L. This is a subgroup of $\mathrm{Gal}(L/K)$ with fixed field K so $H_{|L} = \mathrm{Gal}(L/K)$ thanks to the usual Galois theory for finite extensions. So, there exists $\tau \in H$ such that $\tau_{|L} = \sigma_{|L}$, which means that $\tau \in H \cap \sigma \,\mathrm{Gal}(F/L)$. We just showed that we can approximate any $\sigma \in \mathrm{Gal}(F/K)$ with a certain $\tau \in H$ with any precision we want (by precision we mean $\sigma = \tau \in H$ on arbitrarily big finite Galois extensions of K). So we just showed that σ is in the closure of H. Since H is already a closed subgroup we deduce that $\sigma \in H$ hence $\mathrm{Gal}(F/K) \subset H$. We have thus showed that $H = \mathrm{Gal}(L/K)$ and hence that the map $K \mapsto \mathrm{Gal}(F/K)$ is surjective.

It remains to show that last claim of the theorem. Let H be an open subgroup of $\mathrm{Gal}(F/k)$, which is then also closed and hence of the form $\mathrm{Gal}(F/K)$ for some extension K (this is thanks to the Galois correspondence we have established above). The group $\mathrm{Gal}(F/k)$ is the disjoint union of the open cosets σH, but since it is compact there exists $\sigma_1, \ldots, \sigma_n$ such that $(\sigma_i H)$ is an open covering of $\mathrm{Gal}(F/k)$. We then deduce that the index $[\mathrm{Gal}(F/k) : H]$ is finite. This means that K/k is a finite extension. The converse is fairly clear: if K/k is finite then $\mathrm{Gal}(F/K)$ is an open subgroup. □

Yassine El Maazouz